Combatant Status and Computer Network Attack

SEAN WATTS*

* Assistant Professor, Creighton University Law School; Professor, The Judge Advocate General's Legal Center & School, Army Reserve (DIMA). Although governments highly classify information relating to the topics discussed in this Article, the author relied entirely on publicly available sources in his research. Thanks to Professors Michael Kelly and Eric Jensen for reviewing drafts of this Article. Thanks to Ryann Miller, Emily Cameron, and Pat Anderson for excellent research and technical assistance.

INTRODUCTION

The law of war is largely reactive in nature—a collection of retrospective regulations modeled on past conflicts. Evolutions, and even revolutions, in warfare rarely inspire novel or tailored legal provisions. Instead, legal advisors and international law scholars review innovations in strategy, means, and methods of war under decades- or even centuries-old law and tradition. Applied to conditions of combat unfathomable to its drafters, the law of war often seems dated or ill-equipped for the changes and challenges of modern war.[1] Military legal history has demonstrated that the law of war's efficacy is a function of the law's ability to keep pace with, as well as to address, how war is waged.

Few transformations in war rival, in breadth or import, the impact computers and information networks have had on the conduct of hostilities.[2] Current military strategy regards cyberspace as a domain of war on par with land, air, and sea.[3] States' commitments to computer net-

1. In 2002, lawyers with the Office of Legal Counsel of the U.S. Department of Justice infamously judged the 1949 Geneva Convention III on the Treatment of Prisoners of War "quaint" and ill-equipped to deal with the challenges of U.S. operations against transnational terrorists. *See* THE TORTURE PAPERS: THE ROAD TO ABU GHRAIB 119 (Karen J. Greenberg & Joshua L. Dratel eds., 2005).

2. *See* LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 1 (1998) (noting the pervasive effects of the Information Age on military art); Brian T. O'Donnell & James C. Kraska, *Humanitarian Law: Developing International Rules for the Digital Battlefield*, 8 J. CONFLICT & SECURITY L. 133, 160 (2003) (arguing that digital warfare may eventually eclipse kinetic engagements); *see also* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 886 (1999) (arguing that computer network attacks threaten certain societal values and that the use of force prohibition located in the U.N. Charter does not properly protect against this threat). *See generally* Audrey Kurth Cronin, *Cyber-Mobilization: The New Levée en Masse*, PARAMETERS, Summer 2006, at 77 (arguing that this century is witnessing a *levée en masse* that is mobilized through cyberspace and that Western states must shift their defensive focus); Donald H. Rumsfeld, *Transforming the Military*, FOREIGN AFF., May–June 2002, at 20 (arguing that war is increasingly being waged in nonmilitary ways so the United States must shift the way it fights and trains and must also recognize the importance of preemptive offense).

3. The commander of the U.S. Strategic Command recently equated cyberspace with land, sea, and air as a critical war-fighting domain. *See* Wyatt Kash, *Cyber Chief Argues for New Approaches*, GOV'T COMPUTER NEWS, Aug. 22, 2008, http://gcn.com/articles/2008/08/22/cyber-

work operations have provoked government-wide efforts to adapt national security policy, strategy, organization, and legal authority to achieving security in cyberspace.[4] While efforts appear directed toward defensive measures, there are strong indications that states have developed offensive capabilities, including personnel organized and trained to launch offensive computer network attacks (CNAs).[5]

Not surprisingly, important legal questions emerge from CNAs, provoking extensive debate over the adequacy of the law of war. Existing legal analysis addresses a broad range of issues, from CNA victims' right to resort to force and the lawful use of preemptive or defensive CNAs (so-called *jus ad bellum* issues), to analyses of how the law regulating the conduct of hostilities (the *jus in bello*) applies to CNAs.[6]

---

chief-argues-for-new-approaches.aspx.

4. *See generally* OFFICE OF GEN. COUNSEL, U.S. DEP'T OF DEF., AN ASSESSMENT OF LEGAL ISSUES IN INFORMATION OPERATIONS (2d ed. 1999) (outlining a wide range of legal issues associated with computer network operations).

5. A host of terms in the Department of Defense's (DOD) dictionary of military terms describes the spectrum of operations employing or directed against computer networks during armed conflict and peace. *See* JOINT CHIEFS OF STAFF, JOINT PUBLICATION 1-02: DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS (2009), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. Among the most common terms associated with CNA are "information operations," defined as "integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own," and "information system," defined as "[t]he entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information." *Id.* at 263. The Joint Chiefs of Staff define computer network attacks as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-13: INFORMATION OPERATIONS GL-5 (2006), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. An Air Force lawyer formerly assigned to the U.S. Defense Information Systems Agency adopted the term "information attack" to describe operations in which computer systems are "the object, means, or medium of attack." Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 187 (2006). For simplicity's sake, this Article will use the term CNA in its broadest sense. The term "cyberattack" refers to efforts to destroy or disrupt computer systems. *See* NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens, Kenneth W. Dam, Herbert S. Lin eds., 2009). By comparison, computer network exploitation (CNE) refers to efforts to penetrate systems to gain information on the system and its vulnerabilities, thus acting as a tool for intelligence collection rather than system destruction. *See* CLAY WILSON, INFORMATION OPERATIONS, ELECTRONIC WARFARE, AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES 5 (Cong. Research Serv., CRS Report for Congress Order Code RL31787, Mar. 20, 2007), *available at* http://www.fas.org/sgp/crs/natsec/RL31787.pdf.

6. *See infra* notes 162–85 and accompanying text (suggesting how the law determining combatant status would apply to the participants of a CNA). *See generally* SUSAN W. BRENNER,

While assessments range from conclusions that existing law is largely adequate,[7] to arguments to abandon the extant law entirely,[8] to calls to draft a new *lex specialis*,[9] broad consensus exists that CNAs producing destructive effects fully implicate law-of-war restraints and authorizations, both codified and customary.[10]

CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE (2009) (arguing for better integration of law enforcement and military responses to cybercrime, cyberterrorism, and cyberattacks); Louise Doswald-Beck, *Computer Network Attack and the International Law of Armed Conflict*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 163 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (positing limits that international humanitarian law might impose on CNA); Michael N. Schmitt, *Wired Warfare: Computer Network Attack and the* Jus in Bello, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *id*. at 187 (concluding the existing law of war is generally sufficient to regulate CNA).

7. *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 6, at 99, 114–15 (observing that "it usually dawns on belligerent parties that there is no insuperable difficulty in applying the general principles and rules of international law to the novel weapon," including CNAs); *see also* Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1146–50 (2003) (arguing that, although CNA and computer network operations have expanded the number of available targets and may bring about unexpected tertiary effects, existing laws applicable to all military operations are still adequate).

8. *See* Anthony D'Amato, *International Law, Cybernetics, and Cyberspace*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 6, at 59, 59–61. D'Amato directly refutes Dinstein's approach of applying existing law to CNA. *Id.* D'Amato argues for and predicts a complete immunization of the Internet from hostilities. *Id.* at 68.

9. *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1023 (2007). Professor Hollis relates: "In 1998, states were unresponsive to Russia's request that states devise new international law rules to prohibit particularly dangerous information weapons." *Id.* at 1037 (citing Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General, U.N. Doc. A/C.1/53/3 (1998)); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, at 8, *delivered to the General Assembly*, U.N. Doc. A/54/213 (Aug. 10, 1999)). Hollis notes that "of nine states submitting views, only Cuba and Belarus favored negotiations to restrict information warfare. Ultimately, the U.N. General Assembly passed Resolution 53/70, calling on member states simply to promote consideration of existing and potential threats to information security." Hollis, *supra* at 1037 n.62 (citing G.A. Res. 53/70, at 2, U.N. Doc. A/RES/53/70 (Jan. 4, 1999)).

10. *See* WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 140 (1999). Sharp offers the criteria of scope, intensity, and duration to evaluate whether CNA rise to the level of "use of force," "armed attack," or "armed conflict"—three important thresholds for the application of the law of war. *Id.* at 138. He concludes that CNA are capable of satisfying each criterion, thus triggering relevant law-of-war legal regimes. *Id.* Contrast these criteria with Jean Pictet's analysis of the "armed conflict" threshold of the 1949 Geneva Conventions. *See* COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK ARMED FORCES IN THE FIELD 32–33 (Jean Pictet ed., 1952). Pictet argues for an extremely low threshold such that any difference between states that involves the intervention of armed forces constitutes armed conflict. *Id.* In Pictet's view, "[i]t makes no difference how long the conflict lasts, or how much slaughter takes place." *Id.* The International Committee of the Red Cross, the publisher of Pictet's commentary, appears to have adopted his analysis of the armed conflict

The majority of scholarly attention to operation of the *jus in bello* within CNAs focuses on the application of existing targeting rules, such as the principles of military objective, distinction, proportionality, and unnecessary suffering.[11] CNA targeting presents legal issues as complex as any kinetic strike. However, just as important as the questions of *how* and *against whom* CNAs may be lawfully conducted is the question of *by whom* they may be lawfully executed. As states construct CNA arsenals, the question of how to staff agencies and ministries consistent with international legal obligations becomes important both for states themselves as well as for the individuals who undertake CNA duties.

Predictably, existing legal analysis of CNA staffing focuses on the 1949 Geneva Conventions and their progeny.[12] Long ago, the Conventions incorporated an early test for identifying persons eligible for rights and responsibilities under the law of war, and have since shaped discourse concerning combatant status.[13] Highly respected law-of-war

---

threshold. *See* Int'l Comm. of the Red Cross, How is the Term "Armed Conflict" Defined in International Humanitarian Law? (Mar. 2008), http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/armed-conflict-article-170308/$file/Opinion-paper-armed-conflict.pdf. Michael Schmitt criticizes Pictet's actor-based armed conflict threshold, noting that involvement of armed forces may, especially in the context of CNA, be an inadequate test for applying the law of war. *See* Schmitt, *supra* note 6, at 191. Schmitt proposes that armed conflict sufficient to trigger the Geneva Conventions and their progeny occurs when states take measures, beyond merely isolated incidents, "to injure, kill, damage or destroy." *Id.* at 192.

11. *See, e.g.*, James P. Terry, *The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What Are the Targeting Constraints?*, 169 MIL. L. REV. 70, 90–91 (2001) (arguing that, when identifying lawful targets for CNA, it is imperative to differentiate between civilian and military computer networks, because only networks supporting and contributing to the adversary's war effort are lawful targets); Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1450–51 (2008) (arguing that, although cyberwarfare is more likely to violate neutrality and distinction, current international law should adapt to cyberwarfare and promote its usage over traditional warfare in some situations).

12. *See generally* Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, art. 2, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, art. 2, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, art. 2, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, art. 2, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Protocol II].

13. *See* Richard R. Baxter, *So-Called 'Unprivileged Belligerency': Spies, Guerillas, and Saboteurs*, 28 BRIT. Y.B. INT'L L. 323 (1951); Knut Dörmann, *The Legal Situation of "Unlaw-*

scholars concur that restrictions expressed in criteria for prisoner of war (POW) status under the Third Geneva Convention of 1949 present a significant legal obstacle to the use of civilians to launch CNAs with destructive effects.[14] Given their near unanimity and especially their potential to shape how states organize for cyberwar, these conclusions warrant critical examination.

This Article begins by briefly outlining current state activity in CNA. While details of states' CNA capacity are highly secret, publicly available sources shed light on the rough contours of current state practice. From a broad array of sources, Part I deduces reliable assumptions about states' CNA forces, including a vision for significant participation by civilians. Part II provides a brief outline of relevant international legal frameworks related to the law of war, highlighting important historical origins and development, particularly in relation to combatant and civilian status requirements. A synthesis of widely held legal conclusions in the context of CNAs drawn from these sources follows. Part II concludes by illustrating how the preceding legal analyses would alter or limit states' options to organize for CNAs. Part III recommends a departure from existing approaches and suggests an alternative analytical framework based on interpretive and normative considerations. Part III argues that while well-suited to their original, and still vital, purpose, the Geneva Conventions offer outdated or inapposite assumptions about civilian participation in CNA. Rote, seriatim application of the Conventions' tradition-minded criteria either steers state practice into empty formalism or excessively constrains states' options—both of which are proven to produce only contempt for the law. This Article argues that legal analysis of CNA staffing should focus on only one of the Conventions' enumerated combatant status criteria: the underappreciated criterion of state affiliation. As an irreducible minimum of lawful participation in CNA, state affiliation preserves the spirit and intent of the traditional criteria of combatant status, including the dual principles of distinction and discipline, while offering states workable options to develop capacity for what is perhaps unfortunately, yet inevitably, a new domain of warfare.

To be clear, it is not time to abandon the Geneva Conventions wholesale. As recent conflict shows all too well, states abandon the Conventions' wisdom at their peril. Yet the Geneva Conventions work best when reserved for their core competency: regulating states' treatment of

---

ful/Unprivileged Combatants," 85 INT'L REV. RED CROSS 45 (2003).

14. Doswald-Beck, *supra* note 6, at 172.

the victims of war. While admittedly state-centric, the proposed framework for analyzing combatant status in CNA serves the critical demands of humanity and necessity. In addition to offering a realistic and workable solution to the question of CNA staffing, this Article's theory of lawful combatancy presents a potential approach to combatant status in other emerging forms of remote warfare.

I. STATE CAPACITY FOR COMPUTER NETWORK ATTACKS

On August 8, 2008, Russian armed forces entered the separatist Georgian region of South Ossetia.[15] Simultaneously, Russian aircraft bombed the region and conducted reconnaissance flights over other Georgian territory.[16] In what has become an increasingly common first act of modern armed conflict, an intense campaign of CNAs accompanied the Russian invasion, defacing Georgian government websites and denying web-based communication between the Georgian President and the Georgian population.[17]

Later reports revealed that the CNA campaign had preceded the physical invasion by as much as twenty-four hours and that hackers may have launched computer network probing operations as early as July 20th.[18] Although the CNA timing led many to attribute the attacks to the Russian government, solid evidence remains elusive.[19] To date, publicly available comments by computer security experts have not identified the precise source of the attacks.[20]

The attacks on Georgian computers were similar to widespread denial of service operations[21] unleashed against Estonia in April 2007.[22] Later

15. Michael Schwirtz et al., *Russia and Georgia Clash Over Separatist Region*, N.Y. TIMES, Aug. 9, 2008, at A1 (offering a same-day account of the invasion).

16. Peter Finn, *A Two-Sided Descent Into Full-Scale War*, WASH. POST, Aug. 17, 2008, at A1 (offering expanded, day-by-day accounts of events leading up to the invasion and covering the conduct of the invasion itself).

17. *See* Schwirtz et al., *supra* note 15.

18. John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1; Linton Chiswick, *Cyber Attack Casts New Light on Georgia Invasion*, FIRST POST, Aug. 15, 2008, http://www.thefirstpost.co.uk/45135,features,cyber-attack-casts-new-light-on-georgia-invasion.

19. Chiswick, *supra* note 18.

20. One report suggests servers located in the United States, perhaps controlled by Russia, initiated attacks against Georgian government websites. *Id.*

21. Directed denial of service attacks typically employ networks of slave computers, or "botnets," to inundate target systems with requests for information or service. The outsized requests overload the target system, causing servers to crash. *See* Shawn Waterman, *Who Cyber Smacked Estonia?*, UNITED PRESS INT'L, June 11, 2007, *available at* http://www.upi.com/Security_Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/2/.

22. In April 2007, after the controversial removal of a Russian war hero's statue, Estonian

analysis of each CNA episode revealed evidence that civilians may have played significant roles in the planning and execution of the attacks.[23] Connections between civilians identified with the attacks and the Russian government remain disputed.[24] Still more uncertain is the extent of the Russian government's internal capacity for CNAs.

Limited access to sensitive information frequently hampers unclassified discussions of states' CNA capabilities and staffing. Agencies believed to possess CNA capacity guard their capabilities and doctrine closely to preserve the effectiveness of their methods and tools. Similarly, agencies that employ CNAs deny public access to their organizational schematics and staffing rolls.[25] Nevertheless, publicly available sources permit acceptable estimations of a number of states' CNA capabilities. This Part provides a simple anatomy of offensive computer network operations, presents evidence of current state capacity for CNAs, and outlines how states have or are likely to organize and staff their CNA programs.[26] The assumptions outlined in this Part will form a factual framework for later analysis of the legal questions related to civilian participation in CNA.

---

government websites experienced widespread outages and vandalism. *Id.*; *see also* Tony Skinner, *War and PC: Cyberwarfare*, JANE'S DEF. WKLY., Sept. 19, 2008, at 38 (reporting that only one individual—an Estonian student from Tallinn—has since been arrested for the attacks, despite a widely held belief that the majority of attacks originated in Russia).

23. Noah Schactman, Kremlin Kids: We Launched the Estonian Cyber War (Mar. 11, 2009), http://blog.wired.com/defense/2009/03/pro-kremlin-gro.html. An Internet security consultant speculates that the Russian government employed an organization known as the Russian Business Network to carry out the attacks on its behalf in exchange for immunity with respect to prior criminal acts. *See* Chiswick, *supra* note 18. The consultant describes the Russian Business Network as a "shadowy, St Petersburg-based internet company" that is "believed to control the world's biggest and most powerful 'botnet'—a network of infected zombie computers of a scale necessary to perform destructive cyber-terrorism or cyber-warfare on an entire state." *Id.*

24. Debate still swirls around responsibility for the denial of service attacks on Estonia. Professor Susan Brenner concludes that Russian government involvement is foreclosed by the simplistic nature of the attacks. *See* BRENNER, *supra* note 6, at 5–6 (noting that even Estonian authorities seem to have absolved the Russian government of responsibility, labeling the attacks instead as "cybercrime").

25. *See, e.g.*, John Markoff & Thom Shanker, *Panel Advises Clarifying U.S. Plans on Cyberwar*, N.Y. TIMES, Apr. 30, 2009, at A18. Reports disclose that America's use of cyberweapons is a highly classified secret that the U.S. government has not publicly acknowledged. These reports reveal that American intelligence agencies have initiated operations in which "electronic gear" was modified in order to disrupt opponent's activities or for mere surveillance purposes. *Id.* The lack of clarity regarding U.S. capabilities or usage of cyberattack weaponry has been attributed to the need to keep the opponent uncertain of the severity of an American counterattack. *Id.*

26. It is worth reiterating that the author's deductions on this topic are drawn exclusively from public information. These deductions are only accurate to the extent that the information cited is itself accurate. Readers should not imply reliance on any classified information or access from the author's professional association with the U.S. Army.

A. Anatomy of a Computer Network Attack

CNAs mirror conventional military targeting operations in several important respects. Many military principles that guide kinetic planning and operations translate directly to CNA.[27] Traditional functions such as intelligence gathering, weapon design and acquisition, and attack execution appear to be critical steps in CNA.[28] Similarities to traditional attack operations also permit analogies between the personnel and staff functions performed incident to kinetic attacks and those required to carry out sophisticated CNA.

1. CNA Intelligence Operations

As observed by the military historian Sir John Keegan, intelligence in war has consistently been a key ingredient to battlefield success.[29] George Washington proclaimed that "[t]he necessity of procuring great intelligence is apparent and need not be further argued."[30] Accordingly, modern militaries have long employed specialized military intelligence staffs.[31] In CNA, knowledge of target system details permits attackers to exploit specific vulnerabilities and enhance the CNA's disruptive or destructive effects.[32]

Computer security experts label these cyberintelligence operations "Computer Network Exploitation" (CNE). CNE tools probe target net-

---

27. *See generally* CHAIRMAN OF THE JOINT CHIEFS OF STAFF, NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS (2006), *available at* http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf. This unclassified report is a lengthy but indispensible tool for understanding CNA. Similar to operational speed in combat, speed in cyberspace operations can be a treasured advantage. In cyberspace operations, information travels near the speed of light. Speed can be both an advantage and disadvantage, as it can allow military commanders to deliver operational effects at speeds previously unknown, while also attracting unintended attention and evasive actions due to the rapid tempo of operations. Additionally, the element of surprise is equally important in both kinetic and information warfare operations. *See* Brown, *supra* note 5, at 204–05.

28. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 79–158.

29. *See generally* JOHN KEEGAN, INTELLIGENCE IN WAR (2003).

30. *Id.* at 7.

31. *See* JOINT CHIEFS OF STAFF, JOINT PUBLICATION 2-01: JOINT AND NATIONAL INTELLIGENCE SUPPORT TO MILITARY OPERATIONS (2004), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp2_01.pdf (outlining doctrine for DOD-wide intelligence operations); U.S. DEP'T OF THE ARMY, FIELD MANUAL 2-0: INTELLIGENCE (2004), *available at* http://www.fas.org/irp/doddir/army/fm2-0.pdf (outlining organization of Army intelligence staffing).

32. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 118. Details that are useful to CNA include physical configuration of hardware, Internet Protocol addresses of connected computers, security patch installation histories, target platform operating systems, operator identities, and information on delivery of computer components to the target facility. *Id.*

works to collect information or to identify vulnerabilities.[33] Although the programs used for CNE may resemble CNA tools, they are distinguished in their effects. Rather than disrupt the target system, CNE tools merely collect information and report to their handler.[34] Not all CNE precedes attacks or even signals a future intent to attack, but CNE forms a critical first step to effective network attacks.

Network reconnaissance serves not only operational requirements; the law of armed conflict also requires attackers to gather reasonable information on their targets to ensure attacks do not cause collateral damage and casualties out of proportion to military advantage gained.[35] CNAs present significant dangers of unintended consequences. Attacks have been known to produce indirect effects on connected systems or even to result in "blowback"—the return of destructive effects to the attack instigator.[36] CNA intelligence operations include efforts to predict and prevent such collateral damage.

Yet in some instances indirect effects may be the most desired results of CNAs. Certainly, destruction of information or information systems yields tactical or strategic advantages. But "knock-on" effects such as public impatience, communication disruptions, reduced confidence in infrastructure and government, or simply fear produce significant advantages to an attacker.[37] Predicting indirect effects and second-order repercussions of attacks are the traditional realm of intelligence communities and personnel.[38]

The personnel requirements of CNA intelligence gathering activities resemble those of conventional reconnaissance operations as well. Effective CNA teams likely include persons trained in computer reconnaissance. Rather than actually launching or implanting CNA tools, these staff members' responsibilities might include mapping enemy computer networks for an attack or contingency plan. They may bring background structural knowledge of a target processor, learned from a manufacturer or from personal experience with industry. Or, they may be particularly skilled at identifying entry points, hiding spots, and vul-

33. *See* WILSON, *supra* note 5, at 5.

34. *See id.*

35. *See* Protocol I, *supra* note 12, arts. 51(5)(b), 52(2).

36. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 124.

37. See *id.* at 127; Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1149–50 (2003) (analyzing law-of-war collateral damage rules in the context of CNA).

38. *See* U.S. DEP'T OF THE ARMY, *supra* note 31, at 1-15 to -19 (outlining the responsibility of intelligence forces to assess the post-attack effects of operations).

nerabilities to destructive code while remaining undetected by the target system. In some cases, CNA intelligence gatherers may not be computer programmers. Important information, such as passwords and entry points, might be gathered clandestinely from interaction with human sources as well—so-called human intelligence operations.[39]

While nearly all states' armed forces include branches dedicated to military intelligence, most states also employ well-developed civilian intelligence organizations as part of their national security strategy.[40] Operational integration and information-sharing requirements frequently blur distinctions between military and civilian intelligence communities. Such integration appears to be a key element of CNA intelligence operations.[41]

2. CNA Acquisition and Weapon Design

The weapons of CNA are no exception to the growing complexity of arms design. Computer security experts speculate that programs possessed by states far exceed, in both complexity and capacity, the viruses and worms with which computer users are by now familiar.[42] States' in-

---

39. *See id.* at 6-1. The Field Manual defines human intelligence (HUMINT) as "collection by a trained HUMINT Collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities." *Id.*

40. For example, in the United States, the House of Representatives recently approved an organizational overhaul of the nation's fifteen intelligence agencies and appointed a civilian intelligence czar to oversee their operations. *See* Bill Nichols & John Diamond, *Roadblocks Lifted for 9/11 Intel-Reform Bill*, USA TODAY, Dec. 7, 2004, at 8A.

41. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 47. The report observes that

> [s]ignificant amounts of coordination with multiple parties may be required if and when the U.S. government contemplates the use of cyberattack. Although cyberattacks that are narrowly focused on highly specific objectives may not have much potential for interfering with other ongoing cyber operations initiated by other parties, a sufficiently broad cyberattack might indeed interfere. In such cases, it may be necessary to coordinate among a number of parties, including various U.S. government agencies and allied nations. All of these parties may have various cyber operations underway that might interfere with a U.S. cyberattack on an adversary. In addition, these agencies and nations would likely benefit from the strengthening of their defensive postures that could occur with advance notice of a possible in-kind response.

Id. at 47–48.

42. *See id.* at 44; *see also* Strategic Tech. Office, Def. Advanced Research Projects Agency, The National Cyber Range: A National Testbed for Critical Security Research, *available at* http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf (last visited Dec. 13, 2009) (reporting the development of the National Cyber Range to allow researchers to accelerate technology's transitions and better accommodate the President's Comprehensive National Cyber-Security Initiative by evaluating "leap-ahead" cyberspace technology for government agencies, such as the Department of Defense).

telligence services, treasuries, and influence over private sector production permit a high degree of design complexity and specialization.[43]

Complexity is most apparent in the requirement that CNA tools be specifically adapted to their target, perhaps even "post-launch." CNA weapon designers develop the computer code "payloads" that prey upon target vulnerabilities and produce destructive or disruptive effects.[44] The best CNA designers are thought to be capable of producing remarkably adaptive payloads whose activation can be triggered in milliseconds or delayed for years.[45] Upon introduction to a target system, a complex CNA payload may provide intermittent or even constant feedback to the attacker.[46] Payloads may even be designed to receive instructions to mutate or change their mission either by remote message or upon satisfaction of certain embedded criteria.[47]

Development of these weapons obviously requires highly talented, skilled, and specialized designers. Reports indicate a need to develop proficiency in CNA in only a few individuals, rather than the grand scale seen in traditional combat operations.[48] Unclassified sources suggest that U.S. forces have not integrated CNA into recent military campaigns on any significant scale.[49] Reports indicate that few information

43. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 5–6.

44. *See id.* at 88–89. Computer worms, unlike viruses, do not attach to a "host" file. Instead, they can copy and spread themselves through several computers and files around the world in a matter of hours, later carrying out instructions on when and how to attack targets. *See* John G. Malcolm, Deputy Assistant Att'y Gen., Statement Before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census (Oct. 21, 2003), *available at* http://www.usdoj.gov/criminal/cybercrime/Malcolmtestimony091003.htm.

45. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 88–89. For an example of a possible payload embedded in a CNA attack, see U.S. GEN. ACCOUNTING OFFICE, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS 22–25 (1996), *available at* http://www.gao.gov/archive/1996/ai96084.pdf (describing the 1994 attack on the Air Force Rome Laboratory in New York). The Rome attack involved the use of Trojan horses and sniffers to control the laboratory's operational network system. Air Force Information Warfare Center officials speculate that the hackers may have intended to install malicious code that could be activated years later, which could directly affect a weapons system and the safety of the soldiers or pilots who operate that system.

46. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 88.

47. *See id.* at 89.

48. *See, e.g.*, *id.* at 185.

49. CLAY WILSON, INFORMATION OPERATIONS, ELECTRONIC WARFARE, AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES 5 (Cong. Research Serv., CRS Report for Congress Order Code RL31787, Mar. 20, 2007), *available at* http://www.fas.org/sgp/crs/natsec/RL31787.pdf (citing Elaine Grossman, *Officials: Space, Info Targets Largely Cobbled On-The-Fly for Iraq*, INSIDE THE PENTAGON, May 29, 2003, at 1, *available at* 2003 WLNR 92145). Wilson observes that, "during Operation Iraqi Freedom, U.S. and coalition forces reportedly did not execute *any* computer network attacks against Iraqi systems. Even though comprehensive IO

operations experts currently serve as active duty soldiers.[50] Many private companies have employed the skills of those with expertise in the various weapons commonly used in CNA. For example, Panasonic hired a formally convicted computer hacker to monitor its cybersecurity.[51] The government has also hired cybercriminals as "cyberwarriors" or for defensive purposes.[52] Additionally, many of the individuals who conduct CNA attacks have been recruited from various disciplines within the military, including intelligence, operations, and communications.

3. CNA Execution

Finally, CNAs, like their kinetic cousins, require operators or "triggermen." Someone on the attacking end must process the intelligence input, translate political and strategic goals into decisive action, select the appropriate weapon or tool, and actually launch the virus or other destructive code. While launch might merely involve hitting "Send" or "Enter," some sources speculate that sophisticated CNA tools are not merely "fire and forget" weapons.[53] Very few details are available publicly on CNA execution. Available sources, however, identify two particularly important aspects of CNA execution: adaptability and integration.

Complex attacks require oversight and manipulation by operators, often in real time. CNA operators must be particularly adaptive, monitoring attacks in progress and responding to unforeseen obstacles.[54] Such obstacles include firewall protection that deflects routine attacks on computer networks. In response, CNA operators "have adopted stealthier, more focused techniques that target individual computers through

---

plans were prepared in advance, DOD officials stated that top-level approval for several CNA missions was not granted until it was too late to carry them out to achieve war objectives." *Id.* (emphasis added).

50. *See* Andrew Koch, *New Powers for Info Operations Chiefs*, JANE'S DEF. WKLY., Sept. 17, 2003, at 6.

51. Natasha Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 301 (2008).

52. *Id.* (citing Jonathan Wolf, *War Games Meets the Internet: Chasing 21st Century Cybercriminals with Old Laws and Little Money*, 28 AM. J. CRIM. L. 95, 104 (2000)).

53. NAT'L RESEARCH COUNCIL, *supra* note 5, at 120.

54. *Id.* at 185; *see also* CHAIRMAN OF THE JOINT CHIEFS OF STAFF, *supra* note 27, at 11 (emphasizing the importance of command and control (C2) in cyberspace operations). *Strategy for Cyberspace Operations* defines C2 as "achieving unified action vertically and horizontally, among all levels of war, and throughout organizations." *Id.* It also notes that, "[d]ue to the nature of cyberspace, C2 requires extremely short decision-making cycles . . . at the speeds required for achieving awareness and generating effects." *Id.*

the world wide web."[55] The flexibility and discretion required by CNAs suggest human input is important throughout. Only highly trained operators seem capable of such nuanced tasks. For example, individuals proficient in software programming, signaling command and control (C2), protocol architecture, or encryption possess the skills to administer malicious code into hardware, software, firmware, and encryption mechanisms within vulnerable technology.[56]

Adding to the difficulty, cyberattacks occur in interconnected and complex environments. Often, the same pathways used to conduct peaceful and routine operations serve as the conduits for highly destructive CNAs.[57] Despite the need for surprise and secrecy, successful CNAs must be integrated and highly coordinated events. Sources indicate that persons responsible for executing CNAs must coordinate with domestic and international agencies, and perhaps with private enterprises, to minimize both undesired indirect effects and well-intentioned, friendly interference.[58]

Once launched, CNAs are capable of producing disturbingly destructive effects. It is widely understood that CNAs may be used to destroy information residing on target systems. Yet the capacity of CNAs to disrupt the functions of computers and networks that control vital services or harness potentially destructive forces, such as hydroelectric dams or nuclear power plants, likely represents their greatest security threat. The former U.S. Director of National Intelligence recently equated the potential fallout from modern CNAs to that produced by weapons of mass destruction.[59] A 2007 U.S. Department of Energy exercise confirmed

55. SYMANTEC, INTERNET SECURITY THREAT REPORT EXECUTIVE SUMMARY: TRENDS FOR JULY–DECEMBER 07, at 2 (2008), *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf.

56. CHAIRMAN OF THE JOINT CHIEFS OF STAFF, *supra* note 27, at D-1. Hackers use common means to administer malicious code, potentially presenting catastrophic results. For example, government officials have received targeted e-mails containing portable document format (PDF) documents with hidden destructive payloads. Once opened, code installs backdoor Trojan viruses on the user's computer to install a toolkit program system, called GHOST. During these attacks, the GHOST system can be used to collect sensitive information found on the user's computer screen. William Jackson, *Malicious PDFs Exploit Zero-Day Vulnerability and Adobe Reader*, GOV'T COMPUTER NEWS, Feb. 20, 2009, http://gcn.com/Articles/2009/02/20/PDF-zero-day-exploit.aspx.

57. *See* GREENBERG ET AL., *supra* note 2, at 10 (discussing affiliated complications arising under the international law of neutrality).

58. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 48. *See generally* CHAIRMAN OF THE JOINT CHIEFS OF STAFF, *supra* note 27 (explaining that partner departments and agencies have a role in securing cyberspace for the United States).

59. *See* JOHN ROLLINS & ANNA C. HENNING, COMPREHENSIVE NATIONAL CYBERSECURITY

that a network attack could disrupt electricity generation and delivery on a vast scale.[60] In recognition of their destructive potential it is not surprising that states have embarked on aggressive efforts to add CNAs to their arsenals.

B. State Computer Network Attack Capabilities and Staffing

It is clear that CNAs are no longer (assuming they ever were) the exclusive realm of disgruntled private actors, self-aggrandizing hackers, and enterprising criminals. States appear to be actively developing capacity and organizing agencies designed to carry out complicated CNAs. As the Georgian and Estonian attacks illustrated, CNAs already constitute part of the current international security environment.[61] Although details are few, publicly available sources permit the following conclusions concerning state CNA capacity and staffing.

First, states—both major and minor powers—are developing CNA capacity.[62] A recent report to the U.S. Congress surmised that China, Russia, Cuba, Iran, Iraq, Libya, and North Korea possess or are pursuing CNA arsenals.[63] In 2006, the CEO of a leading cybersecurity firm, speaking at a U.S. Air Force conference, went further, estimating that over twenty countries now have cyberattack programs.[64] A U.S. General Accounting Office (now the Government Accountability Office) estimate dwarfed both figures, asserting that over 120 countries and organi-

---

INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS 3 (Cong. Research Serv., CRS Report for Congress Order Code R40427, Mar. 10, 2009), *available at* http://fas.org/sgp/crs/natsec/R40427.pdf.

60. *Id.* (citing Jeanne Meserve, *Staged Cyber Attack Reveals Vulnerability in Power Grid*, CNN.COM, Sept. 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html).

61. *See supra* text accompanying notes 15–24.

62. *Intelligence Community Annual Threat Assessment: Hearing Before the S. Armed Serv. Comm.*, 111th Cong. 39 (2009) (statement of Dennis C. Blair, Director of National Intelligence), *available at* http://armed-services.senate.gov/statemnt/2009/March/Blair%2003-10-09.pdf; *see also* U.S. GEN. ACCOUNTING OFFICE, *supra* note 45, at 24 (reporting that Air Force officials acknowledged that one of the hackers responsible for the Rome Laboratory attacks in 1994 was possibly working for a foreign country to obtain military research information or data within the Air Force's advanced research areas).

63. *See* WILSON, *supra* note 5, at 10. China is reputed to have formed cyberspace battalions and regiments, commissioned to attack and exploit military, government, and commercial networks. *See* Keith B. Alexander, *Warfighting in Cyberspace*, 46 JOINT FORCE Q. 58, 59 (2007). As confirmation, Alexander reports: "In November 1999, the *PLA Daily* stated . . . that 'it is essential to have an all-conquering offensive technology and to develop software and technology for net offensives . . . able to launch attacks and countermeasures.'" *Id.*

64. Dawn S. Onley & Patience Wait, *Red Storm Rising*, GOV'T COMPUTER NEWS, Aug. 17, 2006, http://gcn.com/Articles/2006/08/17/Red-storm-rising.aspx (citing comments by John Thompson, chairman and chief executive officer of Symantec Corporation).

zations possess information warfare assets.[65] As evidence, state actors appear to have initiated recent attacks—notably "Titan Rain" and "Moonlight Maze"—against U.S. Department of Defense (DOD) systems.[66] States have allegedly initiated CNAs even against armed forces deployed to combat zones.[67]

In an age where the gap between the "haves" and "have-nots" of conventional armed forces appears to be growing, it is not surprising that states have resorted to CNA as a leveler. In relative terms, CNA tools are far cheaper and easier to develop than conventional arms systems.[68] Moreover, cyberattacks render traditional considerations of military strategy, such as population size and geography, largely irrelevant.[69] States that had previously enjoyed spatial separation from enemies enjoy no such advantage on the CNA battlefield. Glimpses of emerging

65. U.S. GEN. ACCOUNTING OFFICE, *supra* note 45, at 4–5; *see also* John Christensen, *Bracing for Guerrilla Warfare in Cyberspace*, CNN, Apr. 6, 1999, http://archives.neohapsis.com/archives/isn/1999-q2/0041.html (discussing the surprising ease with which any of the 120 countries could launch an attack). In 2009, the White House concluded that the United States must act immediately to combat the increasing frequency of computer network attacks—conducted by both state and nonstate actors—that are intended to compromise, steal, and completely destroy sensitive government information. *See* WHITE HOUSE, CYBERSPACE POLICY REVIEW 1 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (citing *Intelligence Community Annual Threat Assessment*, *supra* note 62, at 39). If the United States fails to act, possible consequences include loss of economic hegemony and military technological advantages. *Id.*

66. *See* WILSON, *supra* note 5, at 10. Wilson's article cites a news piece by Elinor Abreu, which quotes John Adams, chairman of the security consultancy iDefense, describing Moonlight Maze—launched in 1998—as the "largest sustained cyberattack" on the United States. Elinor Abreu, *Epic Cyberattack Reveals Cracks in U.S. Defense*, CNN, May 10, 2001, http://archives.cnn.com/2001/TECH/internet/05/10/3.year.cyberattack.idg/. The attack involved several backdoor programs that allowed hackers to access the computer networks of the Pentagon and other government agencies. *Id.*; *see also* Declan McCullagh, *Feds Say Fidel Is Hacker Threat*, WIRED NEWS, Feb. 9, 2001, http://www.wired.com/news/politics/0,1283,41700,00.html (reporting the possibility of a cyberattack launched by Cuba). The "Titan Rain" series of attacks involved hackers, reportedly from China, who targeted victims ranging from NASA to the World Bank by installing back door programs. Nathan Thornburgh, *The Invasion of the Chinese Superspies (And the Man Who Tried to Stop Them)*, TIME, Aug. 29, 2005, *available at* http://www.time.com/time/magazine/article/0,9171,1098961-1,00.html.

67. *See* Anna Mulrine, *Computer Virus Hits U.S. Military Base in Afghanistan*, U.S. NEWS & WORLD REP., Nov. 28, 2008, *available at* http://www.usnews.com/articles/news/iraq/2008/11/28/computer-virus-hits-us-military-base-in-afghanistan.html. Attributed to Chinese sources, the attack was launched from thumb drives scattered in locations frequented by U.S. troops who inserted them into DOD computer systems, thus spreading the destructive code. *Id.* The DOD no longer permits the use of thumb drives on its computer systems. Noah Schactman, *Under Worm Assault, Military Bans Disks, USB Drives*, WIRED NEWS, Nov. 19, 2008, http://www.wired.com/dangerroom/2008/11/army-bans-usb-d/.

68. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 69.

69. *See id.* at 22.

military thought confirm states' future intent to leverage the advantages of information warfare against powers enjoying conventional military superiority, such as the United States.[70] Awakening to such competitor state strategies, the United States appears to be in the early stages of a comprehensive effort to contest dominance of cyberspace.[71]

C. United States' Government Organization for Computer Network Attack

Secrecy frustrates efforts to describe in detail the structure of the United States' CNA apparatus.[72] Nevertheless, recent public statements, studies, and procurement efforts permit reasonable assumptions concerning U.S. intentions to develop CNA capacity and to organize agencies responsible for conducting CNA.

The executive mandates of several U.S. federal agencies suggest involvement in responses to and use of CNA. In addition to the DOD and its subordinate intelligence agencies (including the National Security Agency (NSA)), the Department of Homeland Security, the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI) share responsibility for defending against and responding to national security threats.[73] Recently, President Barack Obama announced the creation of a National Cybersecurity Advisor (cyber czar) with regular access to the President and responsibility for coordinating protection of U.S. information networks.[74] A report on cyberspace policy accompanied the President's announcement, outlining intentions to streamline federal government CNA response mechanisms.[75] The report concludes that existing responsibility and authority to conduct responses to cybe-

---

70. QIAO LIANG & WANG XIANGSUI, UNRESTRICTED WARFARE (1999), *available at* http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf. Written by two colonels of the Chinese People's Liberation Army, this book argues that weaker military powers should expand their war planning to untraditional battlefields such as commercial and information forums. *Id.* at 12.

71. *See generally* CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

72. Bemoaning excessive secrecy, a National Research Council report observes that "[s]ecrecy has impeded widespread understanding and debate about the nature and implications of U.S. cyberattack." NAT'L RESEARCH COUNCIL, *supra* note 5, at 28.

73. Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 app. at 542–51 (2006).

74. *See* Ellen Nakashima & Brian Krebs, *Obama Says He Will Name National Cybersecurity Adviser*, WASH. POST, May 30, 2009, at A5.

75. *See* WHITE HOUSE, *supra* note 65.

rattacks and threats is too dispersed, residing in a confusing collection of federal agencies and departments.[76]

Consistent with at least a decade of U.S. practice, the report is entirely silent about U.S. offensive CNA capabilities.[77] Yet, as early as 2003, public documents indicated that the United States was developing guidance on the use of CNA.[78] The recently declassified, though moderately redacted, *2006 National Military Strategy for Cyberspace Operations* indicates that the DOD will use "the full range of military operations" and "may conduct cyberspace operations across national boundaries."[79] Additionally, it appears that prior to announcing the cyber czar position, the Pentagon finalized plans for a cyber command.[80]

The new Cyber Command would appear to alter the military's preexisting structure under the U.S. Strategic Command (STRATCOM).[81] Presently, U.S. CNA capabilities and authority are believed to be shared

---

76. *Id.* at 23.

77. A preexisting document outlined U.S. policy but maintained a distinctively defensive approach. *See* U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf. A presidential directive elaborated on the strategy, yet mirrored its defense-minded approach. *See* Directive on Critical Infrastructure Identification, Prioritization, and Protection, 39 WEEKLY COMP. PRES. DOC. 1816 (Dec. 17, 2003).

78. *See* Bradley Graham, *Bush Orders Guidelines for Cyber-Warfare*, WASH. POST, Feb. 7, 2003, at A1 (describing instructions issued through National Security Presidential Directive 16 calling for guidance on how the United States would use CNA against enemy computer networks). The article indicates that development of the response to the directive has involved a number of agencies including the DOD, CIA, FBI, and NSA. *Id.*

79. CHAIRMAN OF THE JOINT CHIEFS OF STAFF, *supra* note 27.

80. In mid-2009, reports indicated that the President would establish the Command by means of a classified order. David E. Sanger & Thom Shanker, *Pentagon Plans New Arm to Wage Cyberspace Wars*, N.Y. TIMES, May 29, 2009, at A1. Meanwhile, the Air Force announced the formation of "a Numbered Air Force for cyber operations within Air Force Space Command" in mid-2008. U.S. Air Force, Air Force Senior Leaders Take Up Key Decisions (Oct. 7, 2008), http://www.af.mil/news/story.asp?id=123118700. This unit was activated on August 18, 2009, as the 24th Air Force, which will "provide combat-ready forces trained and equipped to conduct sustained cyber operations, fully integrated within air and space operations." U.S. Air Force, 24th Air Force Activated, 2 Units Realign in Joint Ceremony (Aug. 18, 2009), http://www.af.mil/news/story.asp?id=123163831.

81. STRATCOM was created in 1992 for stabilization in the post-Cold War world. In 2002, Secretary Rumsfeld announced that STRATCOM would merge with the U.S. Space Command. Headquartered at Offutt Air Force Base in Nebraska. STRATCOM's missions are "to deter attacks on U.S. vital interests, to ensure U.S. freedom of action in space and cyberspace, to deliver integrated kinetic and non-kinetic effects to include nuclear and information operations in support of U.S. Joint Force Commander operations, to synchronize global missile defense plans and operations, to synchronize regional combating of weapons of mass destruction plans, to provide integrated surveillance and reconnaissance allocation recommendations to the [Secretary of Defense], and to advocate for capabilities as assigned." U.S. Strategic Command, http://www.stratcom.mil/ (last visited Dec. 13, 2009).

by the NSA, a vast intelligence gathering agency organized under the DOD,[82] and STRATCOM, which claims authority to conduct "response actions, including threat neutralization, with respect to cyberattacks against DOD installations."[83] Within STRATCOM, the Joint Functional Component Command for Network Warfare (JFCC-NW) appears to be the lead organization for CNA.[84] Interestingly, the commander of the JFCC-NW is the director of the NSA, perhaps facilitating intelligence support for cyberattacks.

Military officers have identified potential pitfalls in the complex organizational structure of CNA organizations like the JFCC-NW.[85] Reports indicate internal strife over a proposal to affiliate the new Cyber Command with the Air Force. Reportedly, some favor a leading CNA role for the NSA due to its superior intelligence gathering apparatus.[86] Nonetheless, reports of these struggles further confirm the existence of U.S. CNA capabilities.

Regardless of the outcome of internecine struggles, the multiple agencies charged with defending the United States from and responding to cyberthreats make interagency cooperation in CNA highly likely. Therefore, the range of government agencies likely to be called upon in an interagency response to CNA includes agencies not designated "armed forces" by U.S. national authority.[87] For example, interagency intelligence sharing and coordination form a central part of U.S interagency and joint operations doctrine.[88] Notably, agencies such as the CIA

82. The NSA's mission is "to protect U.S. national security systems and to produce foreign signals intelligence information." National Security Agency Home Page, http://www.nsa.gov/ (last visited Dec. 13, 2009).

83. NAT'L RESEARCH COUNCIL, *supra* note 5, at 203.

84. *See* U.S. Strategic Command, Functional Components, http://www.stratcom.mil/functional_components/ (last visited Dec. 13, 2009). The JFCC-NW is one of eight functional component commands organized under STRATCOM. *See id.*

85. Susan E. Magaletta, Command Relationships of Cyberspace Forces (Apr. 2008) (unpublished paper for completion of U.S. Air Force Air Command and Staff College), *available at* http://tinyurl.com/magaletta (outlining concerns regarding command structure and interagency support in cyberspace operations).

86. NAT'L RESEARCH COUNCIL, *supra* note 5, at 132.

87. *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1982). Title 10 of the U.S. Code includes authority to organize and regulate the U.S. armed forces. Other government agencies' respective U.S. Code titles provide similar authority for executive branch agencies. For instance, Title 50 organizes employees of federal intelligence agencies.

88. *See* JOINT CHIEFS OF STAFF, 1 JOINT PUBLICATION 3-08: INTERAGENCY, INTERGOVERNMENTAL ORGANIZATION, AND NONGOVERNMENTAL ORGANIZATION COORDINATION DURING JOINT OPERATIONS vii (2006), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp3_08v1.pdf. The appendix to Joint Publication 3-08 lists fourteen government agencies with whom DOD envisions interacting during operations. JOINT CHIEFS OF

and FBI, which are not part of the armed forces, employ a wide array of government civilian employees and private contractor personnel.[89]

Finally, budget and procurement documents evince U.S. efforts to acquire the tools of CNA. The DOD budget for fiscal year 2008 included a request for "the demonstration of offensive cyber operations technologies allowing attack and exploitation of adversary information systems."[90] A second request in 2008, entitled "Applied Research on Command, Control, and Communications," requested nearly twelve million dollars for cyberoperation technology.[91] Additionally, the Air Force solicited development of the capability for gaining access to "any remotely located open or closed computer information systems; obtaining full control of a network . . . and maintaining an active stealthy but persistent presence within the adversaries' information infrastructure."[92] Not to be relegated to irrelevance, the U.S. Army, in 2007, solicited bids for a network disruption technology that uses "subtle, less obvious methodology that disguises the technique used; protecting the ability whenever possible to permit future use."[93]

Such requests appear to confirm the development of CNA capacity but are unlikely to conform to traditional procurement models where designers and producers merely deliver equipment. The complexity of CNA tools and the demands of CNA operations make a continuing relationship more likely between the private firms and contractors responding to bids for CNA tools and government personnel who will deploy the tools. As outlined above, civilian designers and contractors are likely to participate in a much more direct and ongoing fashion to CNA operations than conventional weapons designers.

STAFF, 2 JOINT PUBLICATION 3-08: INTERAGENCY, INTERGOVERNMENTAL ORGANIZATION, AND NONGOVERNMENTAL ORGANIZATION COORDINATION DURING JOINT OPERATIONS A-1 (2006), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp3_08v2.pdf.

89. John Lasker, *U.S. Military's Elite Hacker Crew*, WIRED NEWS, Apr. 18, 2005, http://www.wired.com/politics/security/news/2005/04/67223. Lasker asserts that organizations responsible for U.S. CNA efforts include personnel from the NSA, the CIA, and the FBI, as well as civilians and military representatives from U.S. allies. *Id.*

90. *See* NAT'L RESEARCH COUNCIL, *supra* note 5, at 234 (citing DEF. TECHNICAL INFO. CTR., EXHIBIT R-2, RDT&E BUDGET ITEM JUSTIFICATION: ADVANCED TECHNOLOGY DEVELOPMENT (2007), *available at* http://www.dtic.mil/descriptivesum/Y2008/AirForce/0603789F.pdf) (requesting over eight million dollars for items entitled "Advanced Technology Development" and "Battlespace Information Exchange").

91. *See id.*

92. *See id.* at 186.

93. U.S. Dep't of the Army, Broad Agency Announcement: Army Offensive Information Operations Technologies 6 (May 3, 2007), *available at* http://tinyurl.com/ArmyOIOT.

Thus, publicly available sources make reasonable the assumption that the United States and other states possess CNA capabilities and that they likely employ a diverse array of agencies, both civilian and military, to conduct such operations prior to initiation of or during ongoing armed conflict. Other states also appear to share the United States' complex CNA personnel architecture, employing civilians at many stages of operations.[94] For example, the Georgian National Security Council Chief, Eka Tkeshelashvili, has suggested a hierarchy within Russian CNA capacity:

> At the top of the hierarchy are the "Soldiers": the professional planners, computer scientists, engineers, and other implementers, including the military itself. Next are what some call the "Mercenaries." These are criminal organizations paid to carry out certain elements of the attacks. In this case, there are strong signs implicating an outfit known as the Russian Business Network (RBN). And, finally, there are the "Volunteers." These are individuals with PC's [sic] who are recruited to carry out attacks. They are provided with access to all the necessary software tools, as well as to detailed instructions for carrying out the attacks.[95]

For purposes of unclassified analysis, this Article therefore will assume a scenario wherein agencies and ministries of governments, not organized as armed forces, employ civilians to plan, directly support, and employ data stream CNA capabilities in support of international armed conflict. [96] A number of important legal questions follow: foremost, what national and individual consequences attend such civilian participation in CNA?

II. THE GENEVA TRADITION AND COMBATANT IMMUNITY

Despite lingering ambiguity concerning states' CNA capabilities, a broad range of commentators accepts that CNAs between states could constitute armed conflict of sufficient scale and intensity to trigger the

94. *See* Shachtman, *supra* note 23.

95. Noah Shachtman, *Top Georgian Official: Moscow Cyber Attacked Us—We Just Can't Prove It*, WIRED NEWS, Mar. 11, 2009, http://www.wired.com/dangerroom/2009/03/georgia-blames/.

96. Scholars have made similar assumptions regarding states' use of civilians in CNA. *See* Schmitt, *supra* note 6, at 197. Schmitt observes that "[s]ome countries have elected to contract out information warfare functions, whether those functions involve the maintenance of assets or the conduct of operations. Moreover, computer network attack is a function that may be tasked to government agencies other than the military." *Id.*

law of war generally and, specifically, the 1949 Geneva Conventions and their 1977 Protocols.[97] The following Part outlines the Conventions' and Protocols' framework for classifying persons, summarizes existing analyses of the framework in the context of CNA, and identifies likely consequences for the CNA personnel staffing schemes outlined in the previous Part.

A. The "Current" Legal Framework

The Geneva Conventions have become nearly synonymous with the law of war. Popular culture often uses the term "Geneva Conventions" as shorthand for the entire body of law that regulates hostilities. The Conventions have surely humanized states' treatment of persons fallen victim to hostilities. Every state has now ratified or acceded to the 1949 Conventions,[98] leading jurists to agree that the Conventions have matured into customary international law.[99] International bodies hold states to the Conventions as a matter of state responsibility.[100] In addition, international criminal tribunals enforce the Conventions against individuals,[101] and a growing collection of universal jurisdiction laws gives the Conventions potential for still broader enforcement.[102] Even domestic

97. *See supra* text accompanying note 10. Scholars debate the boundaries between attacks that constitute cyberwarfare, cyberespionage, cyberterrorism, and cybercrime. *See, e.g.*, BRENNER, *supra* note 6, at 3–56. This Article does not engage this debate, instead relying on the widely-held assumption that a species of CNA produces sufficiently destructive effects to constitute armed conflict.

98. The International Committee of the Red Cross identifies 194 states parties to the 1949 Conventions. *See* International Committee of the Red Cross, The Geneva Conventions, http://icrc.org/Web/Eng/siteeng0.nsf/htmlall/genevaconventions (last visited Dec. 13, 2009).

99. *See* Jean Marie Henckaerts, *Study on Customary International Humanitarian Law: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict*, 87 INT'L REV. RED CROSS 175, 187 (2005) (citing Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257–58 (July 8)). *See generally*, JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (2005) [hereinafter CUSTOMARY INTERNATIONAL HUMANITARIAN LAW]; Theodor Meron, *The Geneva Conventions as Customary International Law*, 81 AM. J. INT'L L. 348 (1987).

100. *See, e.g.*, S.C. Res. 1483, ¶ 5, U.N. Doc. S/RES/1483 (May 22, 2003) (calling "upon all concerned to comply fully with their obligations under international law including in particular the Geneva Conventions of 1949 and the Hague Regulations of 1907") (italics omitted).

101. The Statute of the International Criminal Tribunal for the Former Yugoslavia includes grave breaches of the 1949 Geneva Conventions in the court's substantive jurisdiction. *See* Statute of the International Criminal Tribunal for the Former Yugoslavia, S.C. Res. 827, art. 2, U.N. Doc. S/RES/827 (May 25, 1993).

102. Prior to amendment, Belgian criminal law included a particularly broad implementation of universal jurisdiction. *See* Loi du 16 juin 1993 relative à la répression des infractions graves aux conventions internationales de Genève du 12 août 1949 et aux protocoles I et II du 8 juin 1977, additionnels à ces conventions [Law of 16 June 1993 Relative to the Repression of Grave

U.S. courts, although often hesitant to engage treaties, have enforced the Conventions against the executive branch in times of armed conflict.[103]

Given their relative success at mitigating the horrors of war, it is not surprising that so many jurisdictions apply the Conventions as broadly as possible. Informed audiences, however, increasingly understand that the 1949 Geneva Conventions are only a part of a prolific body of international law that regulates the conduct of hostilities between states and in some cases, though far less prolifically, other forms of armed conflict.[104]

While undoubtedly the most well-known, the 1949 Conventions are actually an iteration of an ongoing tradition of state obligations arising during armed conflict that dates to 1864.[105] The Conventions have been a highly evolutionary body of law, responding to the sufferings of victims of past wars. Yet, as this Part demonstrates, portions of the Conventions incorporate incomplete conceptions of how, and more importantly, by whom modern war is fought.

Breaches of the Geneva Conventions of 12 August 1949 and Protocols I and II of 8 June 1977 Additional to These Conventions], June 16, 1993, Moniteur Belge [M.B.] [Official Gazette of Belgium], Aug. 5, 1993, p. 17751. Spain has also executed a universal jurisdiction statute. *See* LEY ORGÁNICA DEL PODER JUDICIAL [L.O.P.J.] art. 23.4 (Spain), *translated in* LUC REYDAMS, UNIVERSAL JURISDICTION: INTERNATIONAL AND MUNICIPAL LEGAL PERSPECTIVES 183 (2003).

103. *See* Hamdan v. Rumsfeld, 548 U.S. 557 (2006). In *Hamdan*, the U.S. Supreme Court held that Article 3, common to the four 1949 Geneva Conventions, limited the President's power to convene military tribunals to try persons detained during armed conflict. *Id.* at 631–32. Five Justices concluded that military commissions would not be "regularly constituted court[s]." *Id.* at 632–33. Four Justices determined that the commissions' restrictions on access to information would violate the common Article 3 requirement of indispensible judicial guarantees. *Id.* at 634–35 (plurality opinion).

104. In addition to regulating war between states, each of the four 1949 Geneva Conventions includes one article dedicated to regulating conflict between states and nonstate actors, including civil wars. *See* GC I, *supra* note 12, art. 3; GC II, *supra* note 12, art. 3; GC III, *supra* note 12, art. 3; GC IV, *supra* note 12, art. 3.

105. Three major iterations of the Geneva tradition predated the 1949 Conventions. The first was the Geneva Convention of 1864. Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, Aug. 22, 1864, 22 Stat. 940, 129 Consol. T.S. 361. In 1868, states supplemented the original Geneva Convention, notably extending coverage to naval forces. Additional Articles Relating to the Condition of the Wounded in War, Oct. 20, 1868, 22 Stat. 945, 138 Consol. T.S. 189. In 1906, the Geneva tradition added the Convention of 1906, expanding on protections for the wounded and sick. Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, July 6, 1906, 35 Stat. 1885, 22 Consol. T.S. 144. In 1929, states updated the rules for the wounded and sick and added a convention for prisoners of war. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick of Armies in the Field, July 27, 1929**,** 47 Stat. 2074, 118 L.N.T.S. 303; Geneva Convention Relative to the Treatment of Prisoners of War, July 27, 1929, 47 Stat. 2021, 118 L.N.T.S. 343.

The Geneva tradition's primary purpose has always been to alleviate the suffering of victims of war.[106] Each of the 1949 Conventions identifies a class of protected persons—persons who find themselves by virtue of wounds, capture, or enemy occupation in the hands of their nation's enemy. In short, the 1949 Conventions are a law of capture and custody designed to ensure humane treatment.

Although in some respects timeless, the 1949 Conventions appear in other respects dated. Even the Conventions' approach to their primary function, protecting victims of war, may be showing its age. For instance, the Fourth Geneva Convention apportions the majority of its protections solely on the basis of nationality.[107] In modern armed conflicts, war victims' need for legal protections often has less to do with nationality than in past conflicts, undoubtedly leaving persons in the hands of an enemy outside the scope of the Conventions' protections.[108] Greater evidence of poor aging is also apparent in matters the Conventions have come to regulate more recently.

As a byproduct of their largely successful effort to categorize persons in enemy custody, the Conventions have evolved to categorize persons in wartime more generally. As supplemented by a 1977 Additional Protocol, the 1949 Conventions identify two categories of persons under the law of war: civilians and combatants. Geneva status now dictates not only treatment in custody, but also whether one is susceptible to lawful targeting and, according to some commentators, also prescribes (though in a highly convoluted fashion) who is entitled to participate in hostilities.

1. Civilian Status

Curiously, the 1949 Fourth Geneva Convention for the Protection of Civilians does not include a general definition of the term "civilian."[109]

---

106. *See generally* HENRY DUNANT, UN SOUVENIR DE SOLFÉRINO (Int'l Comm. Red Cross 1986) (1862) (recounting the author's desire to establish a humanitarian organization dedicated to preventing the suffering of wounded war victims).

107. *See* GC IV, *supra* note 12, art. 4.

108. For instance, although captured or wounded in intense combat operations with U.S. forces, a number of fighters detained in Afghanistan in 2001 and 2002 were nationals of states not at war with the United States, including Yemen, Saudi Arabia, and Pakistan. *See* John Diamond, *U.S. Rejects POW Label*, CHI. TRIB., Jan. 28, 2002, at A1 (relating that one hundred of 158 detainees in Guantanamo Bay were Saudi Arabian and seventeen detainees were from Yemen). The Fourth Geneva Convention includes a short section of minimal protections applicable regardless of nationality. GC IV, *supra* note 12, pt. II.

109. This Article does not use the term "noncombatants" to refer to civilians. Traditionally the law of armed conflict has used the term "noncombatants" to refer to a subcategory of mem-

In fact, three decades passed before states crafted the widely accepted expression of civilian status included in 1977 Additional Protocol I to the 1949 Geneva Conventions. Article 50 of the Protocol states: "A civilian is any person who does not belong to one of the categories of persons referred to in Article 4(A)(1), (2), (3), and (6) of the Third Convention and in Article 43 of this Protocol."[110]

Dissatisfaction with Article 50 is understandable. The definition neither describes nor offers affirmative criteria for assigning civilian status. Instead, the article uses a negative definition, assigning civilian status to all persons not members of a class of persons described elsewhere. Shortcomings notwithstanding, the use of a negative definition carries two important implications. First, status under the law of war is bifurcated. That is, by virtue of employing a negative, there are only two statuses available under the law of war. One is either part of the class of persons described in the referenced provisions, or one is part of the class of persons not described—that is, a civilian. Second, a meaningful appreciation of the Protocol's negative definition of the civilian class requires familiarity with the external provisions referenced in Article 50. Most international lawyers concur that these provisions describe the class of "combatants."

2. Combatant Status

Readers expecting a simple definition of the combatant class are certain to be disappointed as well. The most widely accepted definition of the combatant class encompasses several provisions of the Third Convention and Article 43 of the 1977 Additional Protocol I. The referenced provisions are themselves a complex amalgamation of legal provisions spanning nearly a century of positive law. A full understanding of the roots of the Geneva combatant class requires navigation of at least four separate law-of-war instruments. Treatment in reverse chronological or-

---

bers of the armed forces. For instance, Article 3 of the Annex to the 1907 Hague Convention notes that the armed forces may be made up of combatants and noncombatants. Convention Respecting the Laws and Customs of War on Land annex art. 3, Oct. 18, 1907, 36 Stat. 2277, 207 Consol. T.S. 277 [hereinafter 1907 Hague Regulations]. Noncombatants primarily include members of the medical services and chaplains considered part of the armed forces, but may also include armed forces members not organized for combat operations such as unarmed, dedicated supply services. *See* Knut Ipsen, *Combatants and Non-Combatants*, *in* THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICTS 65, 84–88 (Dieter Fleck ed., 1995). Noncombatant designation is typically a matter of organization determined by domestic national authority. *Id.* at 84.

110. Protocol I, *supra* note 12, art. 50.

der showcases both the complexities of the class and the dated origins of its criteria.

In response to perceptions that existing law did not account for or adequately protect the full range of persons fighting in modern armed conflict, 1977 Additional Protocol I developed a new, though highly controversial,[111] definitional framework for prisoners of war (POWs). The Protocol embedded the criteria of its combatant class in this POW framework.

Protocol I defines combatants as, "[m]embers of the armed forces of a Party to a conflict . . . ."[112] Helpfully, a preceding section elaborates the term "armed forces," stating:

> The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict.[113]

The Protocol gives further clues to its conception of the combatant class in a subsequent article. Describing actions during hostilities, Article 44 requires that combatants "distinguish themselves from the civilian population" and "carr[y] arms openly."[114] These requirements serve the important function of facilitating opposing forces' efforts to limit their attacks to combatants. Yet, in a controversial nod to tactics employed by guerilla fighters and insurgents, Article 44 relaxes these groups' distinction criteria when, "owing to the nature . . . [of] hostili-

---

111. *Compare* George H. Aldrich, *Prospects for United States Ratification of Additional Protocol I to the 1949 Geneva Conventions*, 85 AM. J. INT'L L. 1 (1991) (noting that the Reagan administration rejected ratification of Protocol I to convey a firm stance against terrorism), Guy Roberts, *The New Rules for Waging War: The Case Against Ratification of Additional Protocol I*, 26 VA. J. INT'L L. 109 (1985) (arguing that ratifying Protocol I negatively affects humanitarian law by legitimizing types of warfare that were not previously recognized as legitimate), *and* Douglas J. Feith, *Law in the Service of Terror—The Strange Case of the Additional Protocol*, NAT'L INTEREST, Fall 1985, at 36 (arguing that Protocol I's reduction in formal requirements for combatant status will legitimize terrorist activity), *with* Hans Peter Gasser, *The U.S. Decision Not to Ratify Protocol I to the Geneva Conventions on the Protection of War Victims: An Appeal for Ratification by the United States*, 81 AM. J. INT'L L. 912 (1987) (arguing that Protocol I does not give combatant status to terrorists because terrorists are not considered part of "armed forces").

112. Protocol I, *supra* note 12, art. 43(2).

113. *Id.* art. 43(1).

114. *Id.* art. 44(3).

ties," observance is impracticable.[115] Several states declined to ratify Protocol I on the basis of the distinction criteria opt-outs.[116]

As suggested by the definition of "civilian" described earlier, a more widely accepted description of combatant criteria appears in the 1949 Third Geneva Convention. Like its later Protocol, the Convention embeds commentary on the combatant class in a POW classification regime. While the Convention actually enumerates six classes of prisoners of war,[117] recall that the Protocol's negative civilian definition in Article 50 identifies only four of these groups as distinct from the civilian class.[118] The four groups constitute classes of POWs generally acknowledged to take active or direct part in hostilities as combatants. These groups include: (1) members of the armed forces of a party;[119] (2) militia, volunteer corps, and organized resistance movements belonging to a party;[120] (3) armed forces of parties to the Conventions not diplomatically recognized by their enemy;[121] and (4) citizens who respond spontaneously to invasion, the so-called *levée en mass*.[122]

The second enumerated group, "militia, volunteer corps, and organized resistance groups," describes many of the unconventional fighters encountered in the Second World War and generated significant controversy at the Conventions' 1948 Diplomatic Conference. A number of states objected to including resistance movements in the class of POWs.[123] A Conference of Government Experts, held one year prior to

115. *See* COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, 521 (Yves Sandoz et al. eds., 1987) [hereinafter COMMENTARY]. The commentary notes that fifty speakers addressed Article 44 in debate and introduced thirteen amendments to the original proposal. *Id.* Although the United States is not a party to Protocol I, it does not object to most of its provisions. *See generally* Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419 (1987). The United States does not, however, consider Article 44, paragraph 3 reflective of customary international law and specifically objects to its operation against nonstate parties. *See id.* at 425.

116. *See, e.g.*, Letter of Transmittal and Letter of Submittal Relating to Protocol II Additional to the Geneva Conventions of 12 August 1949 (Jan. 29, 1987), *reprinted in* U.S. DEP'T OF THE NAVY, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 306 (A.R. Thomas & James C. Duncan eds., 1999) [hereinafter Letters].

117. GC III, *supra* note 12, art. 4(A). While article 4(B) appears to enumerate two additional classes of POWs in the context of belligerent occupation and in neutral territory, closer examination reveals these to be classes previously enumerated in article 4(A). *See id.* art. 4(B).

118. *See supra* text accompanying note 110.

119. GC III, *supra* note 12, art. 4(A)(1).

120. *Id.* art. 4(A)(2).

121. *Id.* art. 4(A)(3).

122. *Id.* art. 4(A)(6); *see infra* note 224 and accompanying text.

123. II-A FINAL RECORD OF THE DIPLOMATIC CONFERENCE OF GENEVA OF 1949, at 238, 241 (2004). The United States wanted to use only the term "armed forces" because it believed the in-

the Geneva Conventions' Diplomatic Conference, determined that the term "armed forces" should refer only to traditional land, air, and sea forces.[124] The Government Experts also decided to include "voluntary corps which are regularly constituted" and which had been part of the 1929 Geneva Prisoner of War Convention.[125]

Yet at the succeeding Diplomatic Conference, some states proposed extending protection to unconventional fighters or members of resistance movements as long as these groups conducted themselves similarly to volunteer corps.[126] Smaller states like Denmark especially wanted resistance groups to be eligible for POW status because they expected to rely heavily on unconventional fighting organizations during armed conflict.[127] Their efforts to secure relaxed criteria for resistance groups met opposition from stronger states like the United States and the United Kingdom.[128] Ultimately, the drafters reached a compromise by restricting POW status to resistance movements and groups that adhered to four criteria. The final treaty enumerated the conditions as follows: (1) being commanded by a person responsible for his subordinates; (2) having a fixed distinctive sign visible at a distance; (3) carrying arms openly; and (4) conducting operations in accordance with the laws and customs of war.[129]

The extension seems reasonable given that organized resistance groups operated in similar battlefield contexts with the militias and voluntary corps that traditionally observed these criteria. Furthermore, adoption of the criteria would both facilitate opposing forces' efforts to distinguish resistance groups from civilians and would ensure observance of the law of war more generally in the chaotic and very trying conditions of battle.

While they presented a workable solution to a pressing post-Second World War dilemma, the four resistance movement criteria were not at all innovative. In fact, the criteria had appeared nearly half a century earlier in the 1899 Second Hague Convention. Initiated at the behest of Russian Czar Nicholas II, the 1899 Hague Conference convened the

---

tention of the Convention's drafters was to extend protection only to such individuals. *Id.* The United Kingdom was willing to extend protection to some of these unconventional fighters, but only if these groups fulfilled strict criteria in addition to the four criteria to which voluntary corps were already subjected. *See id.* at 237–38.

124. *Id.* at 237.

125. *Id.*

126. *Id.* at 240.

127. *Id.*

128. *Id.* at 238, 241–42.

129. GC III, *supra* note 12, art. 4(A)(2).

world's major powers to codify a series of treaties on hostilities and armaments.[130] Although agreement on some topics proved elusive, the Conference concluded a treaty on land warfare, the Second Convention, and annexed Regulations,[131] with relative ease.[132]

Describing the "qualifications of belligerents," Article 1 of the Hague Regulations asserted that "[t]he laws, rights, and duties of war" apply to armies as well as volunteer corps fulfilling the conditions later incorporated by the 1949 Third Geneva Convention. It is interesting to note that the Hague Regulations employ the criteria to describe belligerents more generally than the Third Geneva Convention. Where the Third Geneva Convention uses the criteria merely to identify militia qualifying for POW status, the Hague Regulations explicitly state that a broader range of war rights and duties attaches to persons who fulfill the criteria. The Geneva tradition did not formally evince such an attachment until its 1977 Protocol addressed targeting and other matters outside the Conventions' focus on the protection of war victims.[133]

Yet like their Geneva successors, the Hague drafters also adopted the four militia criteria from a preexisting instrument. In fact, the criteria made their earliest appearance in the positive law of war in the 1874 Brussels Declaration, nearly eighty years prior to their appearance in the Third Geneva Convention and over one hundred years prior to their incorporation into Protocol I.[134] Although it never entered force as an international legal instrument, later treaties, such as the Hague Regulations, reproduced significant portions of the 1874 Declaration. As with the Hague Regulations, the Declaration's four criteria described uncon-

130. *See* James L. Tryon, *The Hague Conferences*, 20 YALE L.J. 470, 471 (1911).

131. Convention With Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803, 26 Martens Nouveau Recueil (ser. 2) 949 [hereinafter 1899 Hague Regulations]. In 1907, states reconvened and concluded a second series of Conventions at The Hague. *See* Tryon, *supra* note 130, at 478. The 1907 Conference reproduced the 1899 land warfare regulations without significant change as the 1907 Fourth Hague Convention and Annexed Regulations. *See* 1907 Hague Regulations, *supra* note 109.

132. Tryon, *supra* note 130, at 473.

133. Law-of-war commentators note a convergence of the Hague and Geneva legal traditions in 1977 Additional Protocol I. A commentary to the Protocols highlights the need for a more comprehensive civilian protection regime: "The fact that the Hague Regulations were not brought up to date meant that a serious gap remained in codified humanitarian law. This has had harmful effects in many armed conflicts which have occurred since 1949 . . . ." COMMENTARY, *supra* note 115, at 587.

134. *See* Project of an International Declaration Concerning the Laws and Customs of War art. 9, Aug. 27, 1874, 4 Martens Nouveau Recueil (ser. 2) 219.

ventional fighting groups, such as militia, to whom all the laws, rights, and duties of the law of war would apply, not merely POW status.[135]

Thus, a complete understanding of the origins of combatant status reveals remarkable consistency. From 1874 to the present, states have resorted to the four criteria to designate groups intended to compose the combatant class. While controversy still swirls over the amendments offered by Protocol I to further accommodate irregular militias, the four criteria represent a widely accepted irreducible minimum for combatant status.

3. Legal Implications of Status

Some legal implications of status under the law of war are clear. In general, civilians enjoy protection from intentional targeting.[136] Belligerents must distinguish between civilians and combatants, and may direct attacks only upon the latter.[137] It is widely asserted that civilians only forfeit protection from targeting by taking direct part in hostilities and only "for such time" as they do so.[138] By contrast, combatants may be targeted intentionally, not by virtue of their conduct or activities, but rather by virtue of their status as combatants.[139] In the context of cyberwarfare, assuming they can be located and identified, civilians taking direct part in CNAs would certainly be subject to lawful attack.

A second, clear implication of status is qualification for law of war protection. Because states have defined the combatant class by reference to classes of POWs, all persons who qualify for combatant status enjoy the now well-developed regime of protection attendant to POW status. Some civilians are also entitled to POW status and treatment.[140] For instance, contractors and suppliers accompanying armed forces, air crews, and merchant marine crews qualify for POW status if captured.[141] Civilians who fail to qualify for POW status also may be eligible for a com-

135. 1899 Hague Regulations, *supra* note 131, art. 1.

136. Protocol I, *supra* note 12, arts. 48, 51(2).

137. *See id.* arts. 48, 51(4); *see also* 1907 Hague Regulations, *supra* note 109, annex art. 27.

138. Protocol I, *supra* note 12, art. 51(3).

139. States implement the right to attack combatants by issuing rules of engagement to their armed forces. *See, e.g.*, CHAIRMAN OF THE JOINT CHIEFS STAFF, INSTR. 3121.02, STANDING RULES OF ENGAGEMENT FOR UNITED STATES FORCES (May 31, 2000), *unclassified extract reprinted in* INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOCATE GENERAL'S SCHOOL, U.S. ARMY, JA 422, OPERATIONAL LAW HANDBOOK 82 (2009). Rules of engagement declare combatants to be "hostile force[s]." *Id.* at 89. Soldiers may attack groups designated as hostile forces at any time without regard to provocation or threat. *Id.* at 88.

140. GC III, *supra* note 12, art. 4(A)(4)–(5).

141. *Id.*

parably well-developed protective regime by virtue of their nationality.[142]

Other legal implications of law-of-war status are less clear. For instance, the Protocol I, Article 43 armed forces definition quoted above[143] observes that combatants "have the right to participate directly in hostilities."[144] Thus, it is widely accepted that members of the combatant class may not be prosecuted for warlike acts, including killings, that otherwise comply with the law of war.[145] That is, mere participation in hostilities is not an offense chargeable against combatants.[146] But what consequences attend to civilians who participate directly in hostilities? And what consequences attend to states that send civilians into war?

Many conclude that the combatant's right to participate in hostilities is exclusive. Under this view, Article 43, by negative implication, prohibits civilians from directly engaging in hostilities.[147] Some further conclude that direct participation in hostilities by civilians is an individual criminal offense against the law of war—a war crime under international law.[148] For instance, the U.S. government recently employed a provision of the Military Commissions Act of 2006 to charge a Canadian seized in Afghanistan with unlawful participation in hostilities.[149]

---

142. *See* GC IV, *supra* note 12, pt. III (detailing treatment obligations for protected persons); *see also* Derek Jinks, *The Declining Significance of POW Status*, 45 HARV. INT'L L.J. 367 (2004) (arguing that civilian protected-person status offers protection comparable to POW status under the 1949 Geneva Conventions).

143. *See supra* note 113 and accompanying text.

144. Protocol I, *supra* note 12, art. 43(2). Curiously, immunity from prosecution for participation in hostilities was not an enumerated protection for POWs in the 1949 Third Geneva Convention.

145. *See* Ipsen, *supra* note 109, at 81 (observing that "[combatants] shall not be called to account for their participation in lawful military operations").

146. *See* United States v. Khadr, No. CMCR 07-001, slip op. at 5 (Ct. Mil. Comm'n Rev. Sept. 24, 2007) (citing Johnson v. Eisentrager, 339 U.S. 763, 793 (1950) (Black, J., dissenting) ("Legitimate 'acts of warfare,' however murderous, do not justify criminal conviction . . . . It is no 'crime' to be a soldier . . . .")).

147. Lisa L. Turner & Lynn G. Norton, *Civilians at the Tip of the Spear*, 51 A.F. L. REV. 1 (2001) (identifying three groups of civilians common in conflict, the legal status of each, and issues that arise as a result of their presence).

148. *See* Brief of Appellant at 11, United States v. Khadr, CMCR 07-001 (Ct. Mil. Comm'n Rev. July 4, 2007).

149. *See Khadr*, No. CMCR 07-001. In Afghanistan, Omar Khadr allegedly attacked U.S. forces with a hand grenade. Khadr did not use an unlawful weapon, limited the effects of his attack to enemy armed forces, and did not represent himself as a protected civilian while preparing for or conducting the alleged attack. Thus, the only potential conduct for which he might be charged under the law of war concerns his mere participation in combat. At present his case is pending a government-requested delay. *See* U.S. Department of Defense, Military Commissions, Omar Ahmed Khader, http://www.defenselink.mil/news/commissionsKhadr.html (last visited Dec. 13, 2009) (providing all publicly available documents from the Khadr proceedings).

Controversy surrounds the purported offense of civilian participation in hostilities. Civilian participation has been a prominent feature of warfare since at least the nineteenth century.[150] While states have legislated widely on conditions of war since then, positive evidence of an international offense of civilian participation is conspicuously lacking. Although the protective regime of the Geneva tradition clearly anticipates civilian participation in hostilities,[151] no provision clearly prohibits civilian participation in hostilities. Positive provisions of international criminal law, such as the grave breaches regime of the Geneva tradition[152] and the Rome Statute of the International Criminal Court,[153] do not include an enumerated offense of civilian participation in hostilities. Nor has the International Criminal Tribunal for the Former Yugoslavia produced a conviction for the offense, despite widespread civilian involvement in combat during the war that dissolved Yugoslavia. Some commentators, including this author, regard the omission as deliberate—evidence of states' preference to treat the offense domestically rather than commit the matter to international law.[154] To date, only domestic courts have prosecuted the offense as such, and only one case clearly purported to ground the offense in international rather than domestic law.[155]

---

150. *See* David B. Rivkin, Jr. & Lee A. Casey, *The Use of Military Commissions in the War on Terror*, 24 B.U. INT'L L.J. 123, 131–32 (2006) (identifying *franc-tireurs* as an example of unlawful enemy combatants and discussing them in the context of what persons may be tried by a military commission).

151. The Fourth Geneva Convention of 1949 clearly anticipates civilian participation in hostilities. Article 5 of the Convention permits states to suspend or derogate some civilian protections of persons suspected of committing sabotage or otherwise posing a threat to their national security. GC IV, *supra* note 12, art. 5. Protocol I of 1977 also clearly anticipates civilian participation in hostilities by suspending protection of intentional targeting. Protocol I, *supra* note 12, art. 51(3).

152. Each of the four 1949 Geneva Conventions enumerates violations that constitute grave breaches. The Conventions oblige states parties to locate and prosecute or extradite persons who have committed grave breaches of the Conventions. *See* GC I, *supra* note 12, art. 49; GC II, *supra* note 12, art. 50; GC III, *supra* note 12, art. 129; GC IV, *supra* note 12, art. 146. Additional Protocol I also enumerates several grave breaches. Protocol I, *supra* note 12, art. 85.

153. Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90.

154. *See* Mark David 'Max' Maxwell & Sean M. Watts, *'Unlawful Enemy Combatant': Legal Status, Theory of Culpability, or Neither?*, 5 J. INT'L CRIM. JUST. 19 (2007).

155. *Ex parte* Quirin, 317 U.S. 1 (1942). Reviewing German saboteurs' habeas petitions challenging their trial by military commission, the U.S. Supreme Court considered the question of whether conduct of hostilities out of uniform constitutes an offense against the law of war. The Court concluded that the saboteurs were susceptible to trial as "unlawful belligerents" for their disregard of the uniform requirement. *Id.* at 35. Though sometimes cited as support for the offense of "unprivileged belligerency" or "unlawful combatancy," the case is probably better understood as an analysis of the law of war prohibition on perfidy. Perfidy prohibits killing, wounding, or capture by feigning a protected status under the law of war, such as civilian status. *See*

In addition to potential individual criminal consequences, civilian participation in hostilities raises concerns of state responsibility. Classically understood, law-of-war treaties operate as contracts between states. When confronted with breaches of these treaties, states may resort to a number of remedies including diplomatic negotiations,[156] mediation,[157] litigation,[158] sanction by international bodies,[159] and, in extreme cases, treaty suspension[160] or even war. Existing treaty-based definitions of the combatant class thus could be interpreted to restrain individual conduct as well as states' composition of their fighting forces. Such a view interprets the combatant-civilian status regime as not merely a means of classifying individuals for purposes of treatment upon capture, but also as a self-imposed limit on how states organize for combat. States that employ civilians to take direct part in hostilities would be in breach of such limits.

What "lawful participation in hostilities" actually refers to is a matter of great debate and beyond the scope of this Article.[161] It is sufficient here to remark that a broad array of scholars and jurists has discerned meaningful limits on the class of persons whom the law of war considers legitimate members of the combatant class.

Protocol I, *supra* note 12, art. 37. Whether the saboteurs were fighting on behalf of a nation-state was actually not at issue in *Quirin* because the saboteurs clearly acted under orders from the National Socialist regime of Germany. *Ex parte Quirin*, 317 U.S. at 21–22. Baxter produced a compelling critique of this aspect of the *Quirin* decision. *See* Baxter, *supra* note 13, at 330–31.

156. *See Serbs Capture U.S. Soldiers*, BBC NEWS, Apr. 1, 1999, http://news.bbc.co.uk/2/hi/europe/309554.stm (discussing diplomatic negotiations between President Milosevic and the United States to seek the release of U.S. soldiers who were abducted by Serbs in neighboring Macedonia).

157. *See* Protocol I, *supra* note 12, art. 90; President of the Security Council, *Statement by the President of the Security Council*, U.N. DOC. S/PRST/2009/8 (Apr. 21, 2009).

158. Statute of the International Court of Justice arts. 35–36, June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993. The International Court of Justice has competence to hear cases between states, including disputes concerning "any question of international law." *Id.* art. 36(2)(b).

159. U.N. Charter art. 41.

160. Vienna Convention on the Law of Treaties art. 60, May 23, 1969, 1155 U.N.T.S. 331, 8 I.L.M 679 (entered into force Jan. 27, 1980).

161. For a number of years, the International Committee of the Red Cross has attempted to clarify the question of what constitutes direct participation in hostilities. Its efforts culminated recently in a study intended to offer nonbinding guidance. NILS MELZER, INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION UNDER INTERNATIONAL HUMANITARIAN LAW (2009), *available at* http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/direct-participation-report_res/$File/direct-participation-guidance-2009-icrc.pdf.

B. Existing Legal Assessments and Scholarship

Lawyers assessing the question of civilian participation in CNAs resort almost universally to the Geneva POW framework and its four combatant criteria outlined above.[162] Approaches, both traditional and reform-minded, employ the four combatant criteria to evaluate whom states may lawfully commission to participate directly in CNAs.

Tradition-minded analyses appear to be the majority viewpoint on the question of lawful participation in CNAs. In a representative study, Louise Doswald-Beck, formerly Legal Adviser with the International Committee of the Red Cross, concludes that rules guiding combatant classification and privilege should be no different in CNA.[163] She observes: "It could well be . . . that persons who actually undertake CNA would be considered civilians who would have no POW status if captured."[164] Doswald-Beck counsels that states might avoid such issues by incorporating CNA personnel into their armed forces.[165] With the second of the four criteria clearly in mind, she goes so far as to recommend putting CNA operators in uniform in anticipation of capture.[166]

Dean Michael Schmitt, of the U.S. Army Marshall Center, offers a similar assessment.[167] Schmitt concludes that civilians participating in CNAs that actually or could foreseeably result in injury, death, damage, or destruction would be illegal combatants.[168] Like Doswald-Beck, Schmitt cautions that a prudent approach would be to employ only military personnel for CNAs.[169] Others echo Schmitt's recommendation of military incorporation, citing the U.S. Navy's assimilation of the Seabees battlefield construction forces as a historical example.[170]

Building off Schmitt's work, an Air Force lawyer recently commented on state practice concerning the use of civilians to perform functions affiliated with combat.[171] Major J. Ricou Heaton observed that modern state practice interprets the purported prohibition on civilian participation in hostilities narrowly, employing civilian contractors and

---

162. *See supra* notes 117–25 and accompanying text.
163. Doswald-Beck, *supra* note 6, at 171–72.
164. *Id.* at 172.
165. *Id.*
166. *Id.*
167. Schmitt, *supra* note 6, at 198.
168. *Id.*
169. *Id.*
170. Adam Sherman, *Forward unto the Digital Breach: Exploring the Legal Status of Tomorrow's High-Tech Warriors*, 5 CHI. J. INT'L L. 335, 339–40 (2004).
171. J. Ricou Heaton, *Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces*, 57 A.F. L. REV. 155 (2005).

employees to perform functions that might formerly have been regarded as combatant functions.[172] While undoubtedly true, Heaton's observations on state practice confirm the traditional approach to the question. States' manipulation of the direct participation standard to avoid application of the four combatant criteria still confirm the Geneva POW regime as the relevant test.

The enduring force of the Geneva POW criteria is apparent even in reform-minded efforts. Professor Susan Brenner offers a more critical approach to the question of civilian participation in CNAs. Like Doswald-Beck and Schmitt, she acknowledges the Geneva framework and concludes that civilians are likely prohibited from participating in CNAs.[173] Yet Brenner calls for a reassessment of rules governing participation in hostilities in light of the practical realities of CNAs.[174] She predicts an inevitable migration of civilians into the conduct of CNAs. Brenner observes that unlike conventional hostilities, civilians may be especially adept at cyberwarfare.[175]

In order to account for the erosion of the traditional rationale supporting the provisions on participation in hostilities, Brenner hints at the need to adapt the law of war; however, like Schmitt and others, her proposed solution focuses on organizational adjustments to national security institutions.[176] Rather than question the applicability of the Geneva regime, Brenner ultimately recommends formation of a Cyber Security Agency composed of law enforcement, intelligence, and military personnel.[177]

Like Brenner, others identify an inexact fit between CNA and the extant law of war. Davis Brown helpfully notes that the law of war is not "situation-specific."[178] The law of war targeting principles of military necessity, proportionality, and unnecessary suffering govern all uses of force, whatever means employed.[179] Brown goes so far as to recommend a separate CNA Convention. Yet Brown incorporates the four POW criteria wholesale in his proposed convention's definition of combatant.[180] Ultimately, Brown concludes that only members of states'

172. *Id.* at 192–93.
173. BRENNER, *supra* note 6, at 180–81, 196–97.
174. *Id.* at 199.
175. *Id.*
176. *Id.* at 281–301.
177. *Id.* at 255–59.
178. Brown, *supra* note 5, at 180.
179. *Id.*
180. *Id.* app. at 216 (explaining Brown's definition of "combatant").

armed forces or groups meeting the Geneva POW criteria are permitted to conduct CNA.[181]

Finally, in an article addressing civilian participation in hostilities generally, Professor Geoffrey Corn, former Special Assistant to the U.S. Army Judge Advocate General for Law of War, affirms the use of the Geneva criteria to evaluate the scope of permissible civilian functions.[182] He departs from the traditional standard by suggesting that evaluations of lawful participation abandon the direct participation test as a threshold for applying the four combatant criteria in favor of what he terms a "functional discretion test." Corn explains:

> By focusing on the relationship between a proposed civilian function and LOAC [law of armed conflict] compliance, the decisive question is not "does the function amount to direct participation in hostilities," but instead "will the exercise of discretion associated with this function implicate LOAC compliance?" If the answer is yes, the function must be reserved to members of the armed forces.[183]

Put another way, Corn argues that civilians should not be permitted to perform functions regulated by the existing law of war. Left to armed forces governed by military disciplinary systems and steeped in military culture, battlefield functions are less likely to depart from accepted restraints on the conduct of hostilities.[184] Corn's test offers the advantage of looking beyond civilian means of participation and towards more meaningful ends or consequences of civilian acts in conflict.

Corn is innovative in his departure from the direct participation threshold. Yet as he emphasizes throughout his compelling piece, his test remains committed to the Geneva POW criteria. In fact, Corn gives primacy to the traditional Geneva criterion of exposure to a system of internal command and military discipline to evaluate authority to participate in hostilities.[185]

As these analyses demonstrate, the Geneva Conventions' prisoner of war criteria are undoubtedly attractive offerings from the positive law of war on the privilege to participate in hostilities. Lawyers from military,

---

181. *Id.* at 190–91.

182. Geoffrey Corn, *Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions*, 2 J. NAT'L SEC. L. & POL'Y 257 (2008).

183. *Id.* at 287.

184. *Id.* at 289–90.

185. *Id.*

humanitarian, and academic backgrounds all resort to the Geneva Conventions' century-old criteria for evaluating lawful participation in hostilities.

C. Implications for Existing Computer Network Attack Organization

The practical implications of the above legal assessments are momentous yet not well-documented. If the assumptions presented in Part II are accurate, the preceding legal analyses suggest that significant, and likely burdensome, adjustments to existing CNA architecture are necessary. The legal impacts on states' organization for CNAs would likely reach intelligence gathering, design, and execution plans.

As noted above, intelligence gathering plays a critical role in operations during armed conflict.[186] While the law of war does not prohibit intelligence gathering, its provisions recognize that personnel captured while collecting information against an enemy may be tried under domestic espionage laws.[187] However, members of the armed forces captured collecting intelligence while in uniform forfeit none of their immunities for participation in hostilities.[188]

The flipside of intelligence gathering's importance to military operations is that the more valuable and integrated the intelligence contribution is to the targeting process, the greater the likelihood the intelligence gatherer is taking a direct part in hostilities, and therefore is subject to evaluation for combatant status. While not of particular concern to military intelligence gatherers such as scouts, during armed conflict, civilian intelligence gatherers not meeting the four combatant criteria might implicate the legal concerns associated with civilian participation in hostilities.

The argument that intelligence collection, or even intelligence analysis, constitutes taking direct part in hostilities is far stronger when such information increases the destructive effects or lethality of an attack. It is foreseeable that some intelligence operations may in fact cause actual harm to an enemy. U.S. Navy and Air Force lawyers have surmised that

186. *See supra* Part I.A.1.

187. 1907 Hague Regulations, *supra* note 109, annex arts. 29–30.

188. *Id.* annex art. 29. Generally speaking, members of the armed forces captured by enemy forces while engaged in espionage during armed conflict may be treated as spies. *Id.* However, Article 29 of the Annex excludes from espionage any information gathering by uniformed members of the armed forces of parties to a conflict in enemy controlled territory. *Id.*

service as an intelligence agent may constitute direct participation in hostilities.[189]

The United States has traditionally evinced a broad view of what constitutes direct participation in hostilities. In 1999, the U.S. Department of the Army observed that "[e]ntering the theatre of operations in support or operation of sensitive, high Value [sic] equipment, such as a weapon system," may constitute active participation in hostilities.[190] However, in the context of a treaty, the United States has seemingly adopted the notion that taking direct part in hostilities requires acts resulting in actual harm to the enemy. The UN Convention on the Rights of the Child recently added the Optional Protocol on Involvement of Children in Armed Conflict, which prohibits parties from allowing members of their armed forces who are under the age of eighteen to "take a direct part in hostilities."[191] Although the United States has not ratified the base Convention on the Rights of the Child, in 2002 the United States ratified the Optional Protocol on Involvement in Armed Conflict.[192] The United States issued an understanding addressing the term "direct participation" upon ratification.[193]

Under the U.S. view, a computer network reconnaissance specialist who performs such intelligence duties as outlined in Part I.A.1 of this Article may be considered to be the equivalent of a military scout, especially to the extent his work enables an attack that would otherwise have

189. *See* Michael E. Guillory, *Civilianizing the Force: Is the United States Crossing the Rubicon?*, 51 A.F. L. REV. 111, 117 (2001) (citing U.S. DEP'T OF THE NAVY, *supra* note 116). Guillory also references Hays Parks, then Special Assistant to the Army Judge Advocate General for Law of War, now Law of War Chair, Office of the General Counsel, Department of Defense, for the proposition that "the gathering of intelligence" constitutes combatant-like activity. *See id.* at 118 (citing W. Hays Parks, *Air War and the Law of War*, 32 A.F. L. REV. 1, 116–35 (1990) [hereinafter Parks, *Air War*]).

190. Memorandum from W. Hays Parks, Special Assistant for Law of War Matters, U.S. Dep't of the Navy, to the Judge Advocate General, Law of War Status of Civilians Accompanying Military Forces in the Field 4 (May 6, 1999) (on file with author).

191. Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict art. 1, May 25, 2000, 2173 U.N.T.S. 222.

192. *Id.*

193. The understanding states that, with respect to Article 1 of the Protocol,

> [t]he United States understands the phrase "direct part in hostilities" to mean immediate and actual action on the battlefield likely to cause harm to the enemy because there is a direct causal relationship between the activity engaged in and the harm done to the enemy. The phrase "direct participation in hostilities" does not mean indirect participation in hostilities, such as gathering and transmitting military information, transporting weapons, munitions, or other supplies, or forward deployment.

Message from the President of the United States Transmitting Two Optional Protocols to the Convention on the Rights of the Child, S. TREATY DOC. NO. 106-37, at VII (2000).

failed. Further, to the extent he continues to provide such critical intelligence input, especially in real time or on a frequently updated basis, his contribution to the CNA begins to look progressively more like direct involvement in hostilities. The more timely and integrated his work is to those who actually launch or conduct the CNA, the more closely he resembles a military scout or forward artillery observer who directs fire onto an enemy.

Consider also a CNA weapons designer described in Part I.A.2.[194] This civilian employee's job is to write the code used by the CNA "triggerman." He is responsible for all aspects of design of the CNA tool. Such a person might seem analogous to the designers of weapons employed by a traditional soldier. He might be compared to the tank production plant worker who builds main battle tanks. Neither of these latter categories of civilians is traditionally thought of as taking a direct part in hostilities. They are more commonly included in that broad category of civilians supporting the war effort.[195] Although one might argue that "but for" their designing or building the weapon, actual harm would not have resulted to the enemy, their participation is generally too remote from its effects to be considered "direct."[196] The program designer therefore would seem not to be an "unlawful combatant" for his work.

Suppose, however, that instead of building off-the-shelf CNA tools, the programmer designs destructive code, custom-built to the intelligence mapped by the computer reconnaissance expert. Imagine further, that he works closely with the mapper and routinely adjusts or tweaks the code, up to the moment of attack. Such efforts ensure that the CNA leverages the most recent intelligence and produces exactly the attacker's intent, including a minimization of collateral damage and casualties. Like the computer reconnaissance expert, under existing analyses this civilian's status is greatly jeopardized by his activities.[197] The CNA weapon designer also may strain the boundaries of permissible civilian contributions to combat.[198]

---

194. *See supra* text accompanying notes 42–47.

195. *See* COMMENTARY, *supra* note 115, at 619.

196. *Id.*

197. In addition to establishing the causal connection between the civilian's participation in the attack, evaluating whether civilian acts constitute taking direct part in hostilities requires an inquiry into whether the pertinent acts "cause actual harm to the personnel and equipment of the enemy armed forces." *Id.* The answer requires analysis of a broad range of effects and whether each produces actual harm. *Id.* Effects might include degraded service, denial of service, destruction of information, destruction of a computer, destruction of a network of computers, or physically destructive effects. *Id.*

198. Clearly, states' ability to conduct such legal analysis is limited according to their corres-

State practice in CNAs may combine any permutation of the roles considered above. Legal complexities quickly compound when the range of civilian participation considered above occurs during operations producing a spectrum of CNA effects. Further, additional complications arise when the same person performs multiple CNA functions—the same computer operator may indeed develop tools for and perform reconnaissance, design CNA weapons based on such reconnaissance, and ultimately execute and be the trigger-puller for an operation. Yet the concern for civilian participation and combatant status remains. Existing legal analyses strongly suggest that states employing civilians in many of the roles described above would be in breach of limits on civilian participation in hostilities.

To avoid these consequences, states may be tempted to resort to empty formalism. Accounts of uniformed personnel being called to computer terminals to click "Send" to launch destructive CNA planned, designed, and otherwise launched by civilian personnel permeate informal discussions of CNA operations. Likewise, others recount the possibility of simply converting civilian personnel into "armed forces" through formalistic but otherwise empty administrative or legislative acts. While such legal fictions may lend policymakers short-term comfort, they merely paper over a flawed fit between state practice and extant law.

III. DEPARTING FROM THE GENEVA COMBATANT STATUS REGIME

Often frustrating to efforts to humanize war through international law is the fact that state affiliation remains a precondition to both full application of the law of war and to the status at the zenith of its protection: the prisoner of war. Increasingly, humanitarian commentators and organizations advance a vision of international law, freed from sovereigns, that recognizes individuals as actors with distinct international legal personality.[199] Human rights treaties represent the strongest positivist strains of such thought, offering enforcement mechanisms that individuals may pursue against states.

---

ponding ability to accurately predict effects of their attacks. Lack of such ability has been raised as a major concern in development of CNA doctrine. *See* Graham, *supra* note 78.

199. *See* THEODOR MERON, THE HUMANIZATION OF INTERNATIONAL LAW (2006); *see also* Dan E. Stigall et al., *Human Rights and Military Decisions: Counterinsurgency and Trends in the Law of International Conflict*, 30 U. PA. J. INT'L L. 1367 (2009) (arguing that international human rights law has become increasingly relevant due to the expanded role of commanders who now engage in activities that are not combat-related).

The law of war has not followed suit. To fully benefit from the protections of the Third Geneva Convention, not only must a belligerent situate himself in a conflict between states; he must also affiliate, in fairly formalistic terms, with an entity or group aligned with a state. This Part questions the interpretive and normative case for relying on the traditional four combatant criteria as a touchstone for combatant status in CNAs and offers state affiliation as a more effective and pragmatic proxy.

A. Interpretive Considerations

1. The Four Criteria

Despite being a persistent feature of over a century of positive law, the four combatant criteria are at the heart of a thorny interpretive debate. These textually enumerated and attractively clear requirements offer an eye-catching shortcut to understanding POW and combatant status generally. Yet it is not clear that all four criteria apply to all combatants. While the Convention identifies six classes of POW,[200] the four criteria appear only in a subsection describing unconventional belligerents.[201] Neither of the 1949 Convention's POW sections addressing regular armed forces includes the criteria,[202] nor do the two sections describing persons that accompany armed forces,[203] nor the section describing the *levée en masse*.[204]

To be sure, the simplest statutory construction of the article regards the Convention's omission of the criteria in sections describing regular armed forces and other groups participating in hostilities as deliberate. Had states intended the four criteria to operate against regular armed forces or *levées en masse* as combatants, drafters could easily have included the criteria in their respective subsections or in a prefatory paragraph to the entire article.

Yet U.S. operations against the Taliban and Al Qaeda raised the issue of the criteria's relevance to the regular armed forces of states nonetheless. In 2002, lawyers in the U.S. Department of Justice's Office of Legal Counsel (OLC) concluded that the criteria were in fact implied in

200. *See supra* note 117 and accompanying text.
201. GC III, *supra* note 12, art. 4(A)(2).
202. *See id.* arts. 4(A)(1), (3).
203. *See id.* arts. 4(A)(4)–(5).
204. *See id.* art. 4(A)(6).

the term "armed forces."[205] Regular armed forces, the OLC argued, were subject to the four criteria as a precondition to POW status.[206] The OLC lawyers argued that the criteria were an incentive to unconventional forces to comport and organize themselves in a manner consistent with the long-standing practices of regular armed forces.[207] Thus, the OLC concluded, regular armed forces fighting in nondistinctive apparel, as the Taliban reportedly had, would forfeit their combatant and POW status.[208]

Adopting the OLC interpretation, President George W. Bush concluded that captured Taliban forces, although likely the *de facto* armed forces of Afghanistan, did not qualify for POW status because, as a group, they failed to satisfy at least two of the criteria.[209] The President's determination drew significant criticism, especially as U.S. forces in Afghanistan, particularly special operations forces accompanying the Northern Alliance, themselves appeared to strain the distinctive emblem criterion.

Two military lawyers engaged in an interesting debate concerning application of the four criteria, particularly the uniform requirement, to regular armed forces special operations units.[210] In his article on Special Forces, Parks professes not to resolve the issue but presents both sides of the argument. He refers to John C. Yoo and James C. Ho for the proposition that the four Article 4(A)(2) criteria apply to members of the armed forces as a condition precedent to prisoner of war status.[211] In a similar vein, Ferrell concludes that the U.S. position must consider the four Article 4(A)(2) criteria applicable to armed forces and a precondition to prisoner of war status.[212] Ferrell references the 2002 U.S. position with respect to the Taliban for support. He notes that the United States denied the Taliban prisoner of war status under 4(A)(3), which, like 4(A)(1), does not explicitly include the four criteria.[213] Specifically,

205. *See* THE TORTURE PAPERS, *supra* note 1, at 90.

206. *Id.*

207. *Id.*

208. *Id.*

209. *See id.* at 134–35.

210. *See* William H. Ferrell III, *No Shirt, No Shoes, No Status: Uniforms, Distinction, and Special Operations in International Armed Conflict*, 178 MIL. L. REV. 94 (2003); W. Hays Parks, *Special Forces' Wear of Non-Standard Uniforms*, 4 CHI. J. INT'L L. 493 (2003).

211. Parks, *supra* note 210, at 510 n.30 (citing John C. Yoo & James C. Ho, *The Status of Terrorists*, 44 VA. J. INT'L L. 207, 219–20 (2003)).

212. Ferrell, *supra* note 210, at 102.

213. *Id.* at 102–03 (citing sources summarizing legal determinations made in THE TORTURE PAPERS, *supra* note 1, at 136–43; Memorandum from Jay S. Bybee, Office of Legal Counsel, Dept. of Def., to the Counsel to the President, Status of Taliban Forces Under Article 4 of the

Ferrell notes that the DOD denied the Taliban prisoner of war status because the Taliban did not distinguish themselves from the civilian population and did not conduct their operations in accordance with the laws of war.[214] Ferrell also points out that the same DOD General Counsel memorandum states: "[T]he [Third] Convention applies only to regular armed forces who possess the attributes of regular armed forces, i.e. distinguish themselves from the civilian population and conduct their operations in accordance with the laws and customs of war."[215] Parks cites Pictet's Commentary to the Geneva Conventions and Draper for the opposing view.[216]

Curiously, the OLC lawyers did not analyze 1977 Additional Protocol I.[217] Proponents of applying the four criteria to the combatant class as a whole have a much stronger textual case under Protocol I. Defining armed forces and combatants in consecutive articles, the Protocol refers explicitly to the four criteria.[218] And while, for a small class of fighters in limited circumstances, it relaxes the requirements of wearing a dis-

---

Third Geneva Convention of 1949 (Feb. 7, 2002), *available at* http://www.justice.gov/olc/2002/pub-artc4potusdetermination.pdf.

214. Ferrell, *supra* note 210, at 102–03.

215. *Id.* at 103 n.28.

216. Parks, *supra* note 210, at 510 n.29 (citing G.I.A.D. Draper, *The Present Law as to Combatancy*, *in* REFLECTIONS ON LAW AND ARMED CONFLICTS: THE SELECTED WORKS ON THE LAW OF WAR BY THE LATE PROFESSOR COLONEL G.I.A.D. DRAPER, OBE 197 (Michael A. Meyer & Hilaire McCoubrey eds., 1998); COMMENTARY: III GENEVA CONVENTIONS RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 46–47 (Jean Pictet ed., 1960)).

217. The OLC lawyers were likely wary of Protocol I because the United States had not ratified the treaty. Moreover, they probably understood that disagreement over the treaty's qualifications for POW and combatant status formed the basis for U.S. objections to Protocol I. *See* Letters, *supra* note 116, at 306. Still, the United States has long regarded portions of the Protocol as reflecting customary international law, binding on parties and nonparties alike. *See* Memorandum from W. Hays Parks et al. to Mr. John H. McNeill, Assistant Gen. Counsel, Office of the Sec'y of Def., 1977 Protocols Additional to the Geneva Conventions: Customary International Law Implications (May 9, 1986), *reprinted in* THE JUDGE ADVOCATE GENERAL'S LEGAL CENTER & SCHOOL, LAW OF WAR DOCUMENTARY SUPPLEMENT 388, 389 (Sean Watts ed., 2006); Michael J. Matheson, Remarks, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Convention*, 2 AM. U. J. INT'L L. & POL'Y 419, 425 (1987).

218. Protocol I, *supra* note 12, art. 43(1). The Protocol states, in relevant part, that "[t]he armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates" and that "[s]uch armed forces shall be subject to an internal disciplinary system which . . . shall enforce compliance with the rules of international law applicable in armed conflict." *Id.* Article 44 accounts for the remaining two criteria, distinctive emblems and carrying arms openly as follows: "In order to promote the protection of the civilian population from the effects of hostilities, combatants are obliged to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack." *Id.* art. 44(3).

tinctive emblem and carrying arms openly, the Protocol clearly preserves these requirements for regular armed forces.[219]

But, as noted earlier, the Protocol does not share the 1949 Convention's universal ratification by states. In fact, Article 44, which contains the clearest application of the uniform requirement to regular armed forces, is among the most controversial provisions of Protocol I, provoking significant qualifications from states parties and forming the basis of several states' decisions not to ratify the Protocol.[220]

Ultimately, whether one regards the four criteria as a precondition to all combatant classes may be a function of the extent to which one accepts the Protocol as reflective of a customary norm binding state parties and nonparties alike. Yet one need not necessarily abandon the positive law to derive workable criteria for the combatant class. Especially in the context of CNAs, a far clearer textual case can be made for the criterion of state affiliation.

2. The Criterion of State Affiliation

Whatever one's interpretive preference regarding textual application of the four criteria to combatants, the universally accepted law of war has always included one clear and critical precondition to combatant status: state affiliation. Embedded in the Third Convention passage that precedes the four enumerated criteria is the caveat that only groups "belonging to a Party to the conflict" qualify for POW status.[221] In the case of the Third Convention, "Party to the conflict" can only mean a nation state that has ratified the Convention.[222] While states undoubtedly con-

219. *Id.* art. 44(7). Article 44(7) states that "[t]his Article is not intended to change the generally accepted practice of States with respect to the wearing of the uniform by combatants assigned to the regular, uniformed armed units of a Party to the conflict." *Id.*

220. An understanding submitted by the United Kingdom is representative of views limiting the operation of Article 44. The United Kingdom notified states parties that it would only apply the relaxed distinction criteria of Article 44 in conflicts against parties fighting colonial domination and racial apartheid. *See* United Kingdom Reservations to Additional Protocol I to the Geneva Conventions (July 2, 2002), *available at* http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument (last visited Dec. 13, 2009).

In his letter of transmittal to the U.S. Senate, President Ronald Reagan cited the Article 44 relaxation of distinction criteria as an especially objectionable change to the law governing POW and combatant status. *See* Letters, *supra* note 116, at 306.

221. GC III, *supra* note 12, art. 4. The paragraph preceding the four enumerated criteria provides in relevant part that "[m]embers of other militias and members of other volunteer corps, including those of organized resistance movements, *belonging to a Party to the conflict* and operating in or outside their own territory . . . ." *Id.* art. 4(A)(2) (emphasis added).

222. *See id.* art. 2. Common Article 2, so named for its identical appearance in all four of the 1949 Geneva Conventions, restricts application of the Conventions to armed conflict between

ceded an expansion of the POW class to irregular combatants, they retained the requirement that all POWs, and by implication all privileged belligerents, trace their participation back to a state party to the Conventions.[223] State affiliation ensured that persons carrying out hostile acts actually fit within the context of the armed conflict in question, separating out violent individual opportunists and bandits. State affiliation also ensured reciprocity of obligation between combatants.

In fact, the universally ratified law of war admits only one class of combatant not formally aligned with a state: the *levée en masse*.[224] Traditionally understood as a spontaneous inhabitant response to foreign invaders, the *levée en masse* is admitted to the POW class as a concession only to temporal exigencies. Traditionally, the term *levée en masse* captures the citizen who takes up a weapon in response to an invading enemy. The law presumes the *levée en masse* does not have time to align itself formally with the state or to meet any other criteria for POW status and is thus temporarily excused from compliance. Therefore *levées en masse* may fight without distinctive emblems or uniforms. However, the moment they have the opportunity to meet the preconditions of organized groups claiming POW status, most importantly state imprimatur, their failure to do so disqualifies them from protection.

Connoisseurs of Protocol I may point to that instrument's expansion of the POW class as an exception to the requirement of state affiliation. Indeed, one of the Protocol's most significant innovations was to bring an even broader range of unconventional fighters into the protective fold of the law of war. Under the Protocol's new rules, belligerents fighting "colonial domination and alien occupation and against racist regimes" gain POW and combatant status.[225] Through the operation of Articles 43

"High Contracting Parties" and "occupation of the territory of a High Contracting Party." *Id.* Thus, only armed conflict and situations of belligerent occupation between nation states trigger the Conventions.

223. *See* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 39–40 (2004) (citing Military Prosecutor v. Omar Mahmud Kassem and Others, 42 I.L.R 470 (Isr. Mil. Ct. sitting in Ramallah 1969)). Reviewing the status of Arab belligerents affiliated with the Popular Front, the court held that irregular forces must belong to a Party to the conflict. *See Kassem*, 42 I.L.R. at 476–77. "Since no Arab Government at war with Israel had assumed responsibility for the activities of the Popular Front—which was indeed illegal in the Kingdom of Jordan—the condition was not fulfilled." DINSTEIN, *supra*, at 39.

224. GC III, *supra* note 12, art. 4(A)(6); *see also* Heaton, *supra* note 171, at 172.

225. Protocol I, *supra* note 12, art. 1(4). Article 1 serves as the Protocol's triggering mechanism, describing armed conflicts to which the Protocol applies in full. In addition to conflicts between nation states, the Protocol technically operates in conflicts between the latter and anticolonial liberation movements and insurgents fighting against racial apartheid. Article 1 describes qualifying conflicts by reference to the parties involved. The term "Party," as it appears through-

and 44 these groups remain subject to the four traditional criteria, except that in very limited circumstances they may disregard the uniform requirement and arms criteria without consequences to their status.

While doubtless a facial concession to the traditional state monopoly on the legitimate use of force, state practice with respect to Protocol I suggests far less willingness to abandon the state affiliation requirement. First, over forty years after completion, more than thirty states still have not ratified Protocol I.[226] Nonparties include militarily important states, such as the United States, India, Pakistan, Iran, Turkey, and Israel, which object to abandoning the requirement of state affiliation.

Second, after forty years of operation, the Protocol's expansion of combatant status to nonstate actors has not matured into custom. A recent study of customary provisions of the law of war does not include nonstate belligerents fighting colonial occupation or apartheid as combatants.[227] Instead, the study offers the 1949 Convention's traditional definition of members of the armed forces of a party to the conflict.[228] Commentary offered by the study confirms the importance of state affiliation to armed forces—belligerent groups must "fight on behalf of a party to a conflict" to gain combatant status in international armed conflict.[229]

Finally, the Protocol's acceptance of nonstate actors fighting colonial domination or apartheid has not proved to be a statistically or militarily significant class of conflict. Most states with histories of colonial exploits abandoned their colonial territories before or shortly after the Protocol entered force. And although used to some political effect by nonstate actors, state parties have not implemented the Protocol's provision in favor of groups fighting apartheid regimes in any major conflict to date. Instead, states regard the overwhelming majority of conflicts between states and fighters not affiliated with states as subject to the provisions of Common Article 3 of the 1949 Geneva Conventions and Additional Protocol II of 1977—collectively known as the law of Non-International Armed Conflict (NIAC).[230]

---

out the Protocol, likely refers to the groups described in Article 1, including the relevant liberation and antiapartheid movements.

226. *See* International Committee of the Red Cross, State Parties to the Following International Humanitarian Law and Other Related Treaties, http://www.icrc.org/IHL.nsf/(SPF)/party_main_treaties/$File/IHL_and_other_related_Treaties.pdf (last visited Dec. 13, 2009).

227. HENCKAERTS & DOSWALD-BECK, *supra* note 99, at 11.

228. *Id.* at 14–15.

229. *Id.* at 15.

230. GC IV, *supra* note 12, art. 3. *See generally* Protocol II, *supra* note 12.

Where state concessions to the law of war regulating international or state-on-state conflict have been significant, states have ceded relatively little to the law of NIAC. Without the prospect of facing belligerents affiliated with peer competitors, states have consistently resisted efforts to expand the law of NIAC. In fact, most regard the notion of a combatant class as entirely inapposite to NIAC.[231] That the dominant legal regime in hostilities conducted by groups without state affiliation makes combatant status unavailable further confirms state imprimatur as the *sine qua non* of combatant status.

Thus, while ambiguity surrounds treaty-based application of the four criteria to combatants other than militia and organized resistance, state imprimatur stands out as a consistent precondition to universal acceptance into the combatant class.

B. Normative Considerations

While the interpretive case against application of the criteria to the combatant class is unsettled, there are strong arguments for applying the four criteria as a normative matter. The criteria provide a compelling incentive for fighters to conform to the traditional practices of armed forces. While their exact origins are not perfectly clear, on the traditional battlefield the criteria doubtless vindicate humanitarian and other normative concerns. However, the evolution of warfare calls into question the relevance of the criteria as normative preconditions to lawful participation in CNAs.

For most of their history, the Geneva Conventions' four combatant criteria accurately addressed concerns arising from how states actually conducted warfare. The requirement of affiliation with a command hierarchy reinforced that war was not an individual pursuit. The chaos of war can often attract rioters, looters, and other violent elements. The requirement of a command structure both eliminates rogue individual actors from the rubric of war and ensures that states could trace unlawful warlike acts to responsible leaders from whom reparations could be exacted.[232] Military command also ensures that under the uniquely stress-

231. *See* United States v. Pineda, No. 04-232, 2006 U.S. Dist. LEXIS 17509, at *7–8, *12 (D.D.C. Mar. 23, 2006) (holding that the defendant was not entitled to combatant immunity because the Geneva Conventions did not apply to members of the Revolutionary Armed Forces of Colombia, which failed to meet the Geneva Convention's definition of a lawful combatant); *see also* HENCKAERTS & DOSWALD-BECK, *supra* note 99, at 14 (observing that, as a matter of customary international law applicable in noninternational armed conflict, combatant status likely only attaches to "State armed forces").

232. Reparations formed an important part of the early positive law of war. *See* 1907 Hague

ful conditions of battle, combatants would strictly limit their operations to actions that were militarily necessary. The decentralized nature of the traditional kinetic battlefield makes command important in this respect. As the scale of the battlefield grows, armed forces conduct their operations in looser, more diffuse formations. Military command structures, with their strict hierarchies and successions of command, ensure that subunits and subordinates, though geographically separated from leadership, will conduct their operations consistent with the state's overall vision for battlefield success.

The requirement of displaying distinctive emblems reinforces important normative values through the law of war as well. The law of war generally recognizes the principle of distinction between combatants and civilians as its "grandfather principle."[233] Listed alternatively as "distinction"[234] or "discrimination,"[235] in both practice and custom, warriors have long honored and trained their forces to respect the principle. Most frequently, distinction operates through the targeting practices of combatants to restrict attacks to legitimate military objectives and to spare civilians and their property.[236]

Yet distinction also comprises combatants' duty to distinguish *themselves* from civilians. Located apart from the Protocol I provisions related to targeting, Article 44 requires, among other provisions, that combatants "distinguish themselves from the civilian population while

---

Regulations, *supra* note 109, art. 3. Article 3 provides: "A belligerent party which violates the provisions of the said Regulations shall, if the case demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part of its armed forces." *Id.*

233. This distinction's first clear codification appeared in one of the founding documents of the positive law of armed conflict. The Lieber Instructions of 1863 state that, because "the distinction between the private individual belonging to a hostile country and the hostile country itself, with its men in arms," had advanced in the preceding years, "[t]he principle has been more acknowledged that the unarmed citizen is to be spared in person, property, and honor as much as the exigencies of war will admit." Francis Lieber, U.S. War Dep't, General Orders No. 100: Instructions for the Government of Armies of the United States in the Field art. 22 (Apr. 24, 1863), *reprinted in* THE LAW OF ARMED CONFLICTS 3 (Dietrich Schindler & Jiri Toman eds., 4th ed. 2004). The nearly contemporaneous St. Petersburg Declaration of 1868 stated similarly, "the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy." Declaration to the Effect of Prohibiting the Use of Certain Projectiles in Wartime, 11 Dec. 1868, 18 Martens Nouveau Recueil (ser. 1) 474, *translated and reprinted in* THE LAW OF ARMED CONFLICTS, *supra*, at 91.

234. A.P.V. ROGERS, LAW ON THE BATTLEFIELD 7 (2d ed. 2004).

235. Parks, *Air War*, *supra* note 189, at 4.

236. Protocol I provides two prongs to the targeting aspect of distinction. First, combatants must direct their weapons only against specific military objectives. Protocol I, *supra* note 12, arts. 51(4)(a), 52(2). Second, targeting distinction requires that combatants not employ weapons that are inherently incapable of distinguishing between enemy combatants and civilians. *Id.* art. 51(4)(b).

they are engaged in an attack or in a military operation preparatory to an attack."[237] By wearing uniforms or insignia visible at a distance, combatants make possible opposing forces' efforts to distinguish lawful targets from protected civilians, ensuring both effectiveness and a measure of humanity. The requirement of carrying arms openly similarly supports the principle of distinction. Indeed, for most of the nineteenth and twentieth centuries military weaponry was often sufficiently distinctive to clearly set belligerents apart from their peaceful civilian counterparts.

Finally, identifying combatants by the conduct of their operations in accordance with the law of war and their exposure to military criminal jurisdiction ensures a measure of reciprocity. In international armed conflict, states expect to engage forces schooled in the laws and customs of war and thus rely on a measure of reciprocal observance of these norms. The traditional battlefield proved to be an environment of dangerous temptations, placing civilian persons and property at the complete mercy of belligerents.[238] As a criterion for combatant status, subjection to internal military discipline introduced a measure of collective conscience, likely to mitigate the temptation to abuse the innocent. The requirement of law-of-war compliance also incentivized states' efforts to instruct their forces in the law in order to assure their protected status. Military justice systems, with their geographically portable jurisdictional frameworks, flexible charging systems, and emphasis on ensuring good order and discipline provided effective (though admittedly imperfect) checks against the potentially inhumane chaos of war.

Thus, a host of important normative considerations has long counseled application of the four criteria to all combatants on the traditional battlefield if only as a matter of custom. Yet modern armed conflict increasingly exposes the four criteria as a dated or at least incomplete conception of how states wage war. At the time of their first appearance in the 1874 Brussels Declaration, line-of-sight attacks constituted nearly the entire range of combat engagements. Mechanized warfare, which greatly speeded armed engagements and expanded the scale of battle, would not emerge for nearly fifty years. Air attacks existed largely in the imaginations of avant-garde military thinkers, with long range, strategic bombing tactics decades from realization. To be sure, the statesmen that employed the four criteria as prerequisites of combatant status were regulating war as they knew it, not as it would evolve later.

237. *Id.* art. 44(3).
238. *See* Corn, *supra* note 182, at 272.

Today, remote means and methods of warfare, of which CNAs are merely a subset, increasingly dominate military operations. Over-the-horizon engagements pit against one another forces located continents apart. The prospect of capture is greatly reduced. Senior leaders may position themselves literally at arms length from subordinate combatants. And the traditional temptations associated with presence on a battlefield, such as pillage and looting, are greatly reduced in the insulated and comparatively sterile conditions of remote warfare. The implications for the relevance of the four combatant criteria are profound.

First and foremost, remote engagements like CNAs do not provoke concern for erosion of the principle of distinction in the same manner that line-of-sight engagements do. If distinguishing civilians from combatants in close combat required uniforms, distinctive insignia, and the open display of one's arms, remote engagements make the outward appearance of persons launching remote attacks nearly irrelevant. Far more than an individual's or groups' outward appearance, distinction in CNAs demands attention to the actual conduct of an attack. As opposed to conventional attacks, where defenders respond to the combatant himself, CNA victims are more likely to respond to the means or method of attack. CNAs effectively remove the appearance of the combatant-operator from the distinction equation. Indeed, the protection these weapons' standoff distance affords to their operators is one of their chief advantages. Combatants themselves have little impact on distinction in these scenarios.

Second, command remains relevant in CNAs only in a much looser sense. Unlike their kinetic counterparts, cybercombatants are not typically isolated or removed from headquarters and political leadership. The cybercombatant is thus highly unlikely to be forced to make autonomous discretionary decisions without the assistance of leadership and specialized staff.

Finally, in CNAs the requirement that combatants be subject to an internal disciplinary system takes on reduced significance as well. If internal military justice systems were regarded as an essential response to the jurisdictional challenge of regulating the activities of far flung forces, CNAs would rarely, if ever, call for such jurisdictional flexibility. Cybercombat could easily be conducted from domestic territory, where municipal criminal laws attach. In CNAs, the use of civilians not traditionally subject to military criminal jurisdiction presents few if any of the difficulties that inform the traditional precondition of an internal military disciplinary system.

In sum, it is increasingly apparent that the Convention's four criteria represent an outdated and simplistic characterization of the conduct of hostilities, particularly in the context of CNAs. By contrast, the criterion of state affiliation vindicates the still important normative goals of peace, distinction, and discipline, while accurately reflecting state practice.

State affiliation ensures the operation of legal controls on the resort to hostilities in the first place, the so-called *jus ad bellum*. While admittedly an imperfect system, the United Nations Charter system is universally ratified.[239] The UN Charter prohibits threats or uses of force in international relations with only two exceptions.[240] Such action is permitted when approved Security Council measures not involving armed forces are "inadequate" to "maintain or restore international peace and security"[241] or when in the exercise of self-defense.[242] Thus state actors engaged in hostilities are traceable to parties to the international legal system's only, if flawed, means for regulating the resort to armed force.

In addition, state affiliation preserves concern for the principle of distinction in CNAs. If concern for distinction remains in CNAs, it is not with participants in CNAs as much as with their weapons and the appearances generated by an attack. CNAs present disconcerting challenges to the principle of distinction. Faced with a series of CNAs against critical information infrastructure falsely attributed to a neutral civilian server, a victim state could not be expected to hold its fire, kinetic or nonkinetic, for long. At some point, the victim state would almost certainly launch an attack in self-defense to disable the apparent source of the CNAs. Such victims might easily rationalize very liberal rules of engagement with minimal identification requirements, all in the name of force protection. As states in such a conflict leverage the ever-expanding web of civilian networks to facilitate their CNAs, they would necessarily render meaningless any civilian-military distinction in cyberspace. A cycle of such responses could very easily escalate hostilities beyond the scope of the original attack or escalate into a full-scale, kinetic conflict.

Surely CNAs have great capacity to confound their target. Effective CNAs are well-disguised. Thus, the true challenge from CNAs with re-

239. *See* United Nations Member States, http://www.un.org/en/members/index.shtml (last visited Dec. 13, 2009). Currently, the United Nations is made up of 192 member states. *Id.* Ratification procedures are embodied in Article 110 of the UN Charter.

240. U.N. Charter arts. 42, 51.

241. *Id.* art. 42.

242. *Id.* art. 51.

spect to distinction may result not from civilian participation, but rather from efforts to disguise the true source of the attack. CNAs routed through civilian servers or programmed to appear as though they originated from civilian institutions may in fact run afoul of states' duty to bear arms openly in the attack. Exploration of this aspect of CNAs' relation to distinction, however, is better left to a dedicated legal discussion of means and methods in CNAs.

While considerable clarification of distinction in the context of CNAs is required, state affiliation ensures that attacks remain subject to the existing international legal framework. In particular, the war crime of perfidy presents an effective check against CNAs exploiting peaceful or civilian networks as cover. Examining distinction, specifically the duty of those taking a direct part in hostilities to make themselves distinct from civilians, civilian CNA participants do not fail distinction by virtue of intentional perfidy. The intent of states' use of civilians in CNAs is not to take advantage of enemy forbearance in targeting such civilians. More likely economic, training, and recruitment limitations drive the use of civilians in CNAs. Situated far from the battlefield, if cyberwarfare can be said to have a battlefield,[243] civilians participating in CNAs do not present a confused picture to the enemy from the perspective of distinction. The likelihood that state-sponsored CNAs could be misattributed to innocent civilian assets and systems makes distinction of means far more important than distinction of personnel launching attacks.

Finally, state affiliation addresses the need for discipline in warfare. While civilians participating in CNAs are ordinarily not subject to internal military disciplinary systems, the increasingly well-developed legal regimes that prosecute and punish war crimes operate nonetheless and vindicate concerns for discipline and humanity. As outlined above, when adopted by the 1949 Convention the criterion of exposure to an internal disciplinary system as a precondition to combatant status seemed reasonable. International enforcement bodies such as the International Criminal Court did not exist. Moreover, the international community's political will to convene ad hoc tribunals to prosecute war crimes appeared spotty and susceptible to victor's bias. Few, if any, international war crimes enjoyed domestic implementation or incorpora-

243. In describing twenty-first century warfare, Michael Schmitt discusses "battlespace" instead of a "battlefield." *See* Michael N. Schmitt, *The Principle of Discrimination in 21st Century Warfare*, 2 YALE HUM. RTS. & DEV. L.J. 143, 161–62 (1999). Battlespace describes both "virtual and non-linear loci of combat." *Id.* at 161.

tion into states' domestic criminal codes. What enforcement of war crimes law existed was constrained largely to members of armed forces.

Since 1994, the international legal discipline of war crimes has enjoyed a significant revitalization. One hundred and nine states have consented to the jurisdiction of the International Criminal Court.[244] At present nearly a half-dozen ad hoc international tribunals operate with jurisdiction to prosecute or investigate international criminal law.[245] Domestic courts augment the work of international tribunals as well. [246] The law of war increasingly forms part of states' domestic criminal codes.[247] And importantly, civilians are equally susceptible to war crimes prosecution, including crimes under command responsibility[248] and vicarious theories of liability such as joint criminal enterprise.[249]

244. *See* Rome Statute of the International Criminal Court, *supra* note 153.

245. *See, e.g.*, Statute of the International Criminal Tribunal for the Former Yugoslavia, *supra* note 101; Statute of the International Tribunal for Rwanda, S.C. Res. 955, U.N. SCOR, 49th Sess., 3453d mtg., U.N. Doc. S/RES/955 (Nov. 8, 1994). Another resolution established a special tribunal in Lebanon to address terror attacks since October 2004. *See* Statute of the Special Tribunal for Lebanon, S.C. Res. 1757, U.N. Doc. S/RES/1757 (May 30, 2007). Specifically, this reaffirms Lebanon's need to bring to justice the individuals responsible for the assassination of Prime Minister Rafiq Hariri. *Id.*

246. *See* Laura Dickinson, *Government for Hire: Privatizing Foreign Affairs and the Problem of Accountability Under International Law*, 47 WM. & MARY L. REV. 135 (2005). After noting the trend toward privatization in all spheres of international interaction, Dickinson argues that "privatization in the international sphere need not actually result in less accountability." *Id.* at 141. Dickinson argues that, "unlike in the domestic context, legal accountability is actually very difficult to achieve under international law with respect to *either* state *or* private actors. Accordingly, though privatization may take constitutional norms out of the equation domestically . . . no equivalent to that constitutional baseline exists in the international realm." *Id.* Because of the relatively low level of enforcement in international law, "any reduction in accountability likely will not be as great as in the domestic sphere, where the baseline of accountability for government action is far more robust." *Id.*

247. *See* War Crimes Act of 1996, 18 U.S.C. § 2441 (2006) (incorporating war crimes into U.S. domestic law). *See also* Agreement Between the High Representative for Bosnia and Herzegovina on the Establishment of the Registry for Section I for War Crimes and Section II for Organized Crime, Economic Crime and Corruption of the Criminal and Appellate Division of the Court of Bosnia and Herzegovina and the Special Department for War Crimes and the Special Department for Organized Crime, Economic Crime and Corruption of the Prosecutor's Office of Bosnia and Herzegovina, (Dec. 1, 2004), *available at* http://www.sudbih.gov.ba/files/docs/zakoni/en/Registry_Agreement_English_version.pdf (citing UN Security Council Resolution 1503, which recognizes a need to establish a High Representative and special chamber, known as the War Crimes Chamber in the State Court of Bosnia and Herzegovina to prosecute lower or intermediate ranking suspects).

248. *See* Rome Statute of the International Criminal Court, *supra* note 153, art. 28(b).

249. *See* Corn, *supra* note 182, at 261.

CONCLUSION

Still reeling from the devastation of the First World War's unrestricted submarine warfare campaign, eleven formerly allied powers convened the 1930 London Naval Conference,[250] producing the 1930 Treaty of London.[251] The agreement established clear rules for the naval engagement of merchant ships.[252] The treaty did not entirely outlaw attacks on merchant shipping, but did include rules intended to protect innocent passengers and crewmen in the event of an attack.[253]

Despite these innovative legal developments, the outbreak of the Second World War quickly revived the brutal submarine tactics the London Treaty had set out to eliminate. The German U-boat fleet gained notoriety for highly effective attacks on merchant ships supplying the Allied war effort as well as attacks on neutral shipping.[254] At the Nuremberg International Military Tribunal, the Allies charged the former

250. *See* Detlev F. Vagts, *The Hague Conventions and Arms Control*, 94 AM. J. INT'L L. 31, 37 n.31 (2000) (citing RAYMOND G. O'CONNOR, PERILOUS EQUILIBRIUM: THE UNITED STATES AND THE LONDON NAVAL CONFERENCE OF 1930 (1962)). Addressing the same concerns, the 1922 Washington Conference on the Limitation of Naval Armament preceded the London Naval Conference. The Washington Conference produced a treaty, but the treaty failed to enter into force. *See* DOCUMENTS ON THE LAWS OF WAR 169 (Adam Roberts & Richard Guelff eds., 3d ed. 2000).

251. Treaty for the Limitation and Reduction of Naval Armaments, Apr. 22, 1930, 46 Stat. 2858, 112 L.N.T.S. 65 [hereinafter Treaty of London].

252. *Id.* art. 22.

253. British delegates to the 1922 Washington Naval Conference reportedly proffered a ban on submarine warfare against merchant vessels altogether. *See* 18 TRIAL OF THE MAJOR WAR CRIMINALS AT THE INTERNATIONAL MILITARY TRIBUNAL 317 (1948) [hereinafter NUREMBERG IMT] (citing YAMATO ICHIHASHI, THE WASHINGTON CONFERENCE AND AFTER 80 (1928)). The provision was referred to in drafts as the "Root Resolution," after the American chief delegate to the conference. 18 NUREMBERG IMT, *supra*, at 317. Though not widely ratified, the treaty eventually gained wide acceptance through accession to a 1936 *Procès-Verbal*. Procès-Verbal Relating to the Rules of Submarine Warfare Set Forth in Part IV of the Treaty of London of 22 April 1930, Nov. 6, 1936, 173 L.N.T.S. 353, 3 Bevans 298. The *Procès-Verbal* incorporated, verbatim, the 1930 Treaty of London rules for attacks on merchant shipping. *See* Treaty of London, *supra* note 251. The German National Socialist government was among the thirty-nine States that acceded to the *Procès-Verbal*. *See* THE LAW OF ARMED CONFLICTS, *supra* note 233, at 1146–47 (listing acceding states and dates). Evidence presented at the International Military Tribunal at Nuremberg indicates that the German Navy disseminated these rules to the U-boat fleet in 1938. *See* 18 NUREMBERG IMT, *supra*, at 314. Strong evidence further indicates that many states regarded the *Procès-Verbal* as reflective of customary international law. *See* DOCUMENTS ON THE LAWS OF WAR, *supra* note 250, at 170 (citing Nyon Agreement pmbl., Sept. 14, 1937, 181 L.N.T.S. 137).

254. These figures appear in documents entitled "Extracts from Official British Foreign Office Reports Concerning German Attacks on Merchant Shipping from September 3, 1939 to February 26, 1941." *See* 35 NUREMBERG IMT, *supra* note 253, at 246 (1949) (appearing as Exhibit 641(a)-D).

commander in chief of the German Navy, Grand Admiral Karl Dönitz, with, among other charges, war crimes in violation of the 1936 *Procès-Verbal* rules for attack.[255] The indictment alleged that since 1939 the German U-boat service waged "unrestricted submarine warfare upon all merchant ships, whether enemy or neutral, cynically disregarding" the 1936 *Procès-Verbal*.[256]

In his defense, Dönitz's lawyers also offered interrogatory responses by Fleet Admiral Chester Nimitz of the U.S. Navy.[257] Nimitz related that as commander in chief of the U.S. Navy Pacific Fleet from 1941 to 1945, he had carried out unrestricted submarine warfare against Japan.[258] Nimitz stated that the attacks on Japanese merchant shipping, without the warning required by the London Treaty and *Procès-Verbal*, complied with orders issued by the U.S. Navy.[259] He further confirmed that U.S. submarines did not rescue Japanese merchant seamen when such rescues would have prevented mission accomplishment.[260] In his

255. 22 *id.* at 557 (1948). Dönitz ultimately served as President of the Third Reich following the suicide of Adolf Hitler. Dönitz's predecessor as commander in chief of the German Navy, Grand Admiral Erich Raeder, faced similar charges before the Nuremberg Tribunal. In addition to war crimes, both Raeder and Dönitz answered to charges of aggression and crimes against humanity.

256. *Id.* The prosecutor presented numerous orders of the German High Command instructing U-boats to engage all manner of ships without warning. 5 *id.* at 215–17 (1949). A 1942 conversation between Hitler and Japanese Ambassador Oshima explained: "We are fighting for our existence . . . . For this reason [we] must give the order that in case foreign seamen could not be taken prisoner. . . . U-boats were to surface after torpedoing and shoot up the lifeboats." *Id.* at 219. Prosecution witness Heiseg related a speech by Dönitz while serving as commander-in-chief of U-boats expressing disbelief that German crews would endanger their own ships by rescuing crews of merchant ships. *Id.* at 225. "By doing that, they were working for the enemy, since these rescued crews would sail again on new ships." *Id.*

257. 17 *id.* at 378–81 (1948); 11 *id.* at 108–11 (1949). The interrogatory appears twice in the records of the tribunal. First, it appears as read into the trial record by Krantzbühler. 17 *id.* at 378–81 (1948). Second, it is in the documentary evidence (Document Dönitz-100) presented to the tribunal. 11 *id.* at 108–11 (1949).

258. 40 *id.* at 109 (1949).

259. *Id.* Interestingly, Admiral Nimitz understood unrestricted submarine and air warfare by the United States as reprisals for Japanese tactics. *Id.* at 111. Nimitz's responses to a series of questions, however, evaded labeling U.S. practices as reprisals. *Id.* Nonetheless, the Admiral's final response may effectively have met the accepted definition of reprisal: "The unrestricted submarine and air warfare ordered by the Chief of Naval Operations on 7 December 1941 was justified by the Japanese attacks on that date on U.S. bases, and on both armed and unarmed ships and nationals, without warning or declaration of war." *Id.* At the time, reprisals were widely defined as measures of retaliation adopted to compel an enemy to discontinue violations of the law and usages of war. 2 WHEATON'S INTERNATIONAL LAW 165 (A. Berriedale Keith ed., 7th ed. 1944). The current U.S. Army law of war manual defines reprisal similarly. *See* U.S. DEP'T OF THE ARMY, FIELD MANUAL 27-10, THE LAW OF LAND WARFARE 177 (1956).

260. 40 NUREMBERG IMT, *supra* note 253, at 111 (1949). Admiral Nimitz explained that U.S. submarines' limited passenger capacity and the "known desperate and suicidal character of

argument to the court, counsel for Dönitz quoted directly from the Nimitz interrogatory, emphasizing submarines' limited capacity for rescue.[261] Furthermore, he argued that the tactics of the Allies made the procedures of the *Procès-Verbal* militarily impossible.[262]

The Tribunal acquitted Dönitz of the charge relating to the sinking of Allied merchant ships.[263] With respect to attacks on neutral ships and failure to rescue shipwrecked crewmen, however, the Tribunal found Dönitz guilty of violating the 1936 *Procès-Verbal*.[264] Yet, citing explicitly the Nimitz interrogatories and British Admiralty orders, the Tribunal announced that it would not consider Dönitz's breaches of the law of submarine warfare when determining his sentence.[265] The court's forbearance in sentencing notwithstanding, the Dönitz verdict quickly provoked the ire of military officers and statesmen across the globe.[266]

In addition to perhaps serving as an isolated rebuttal of the victors' justice indictment of the Nuremberg Tribunal, the Dönitz verdict was an important comment on the role of law in regulating armed conflict. The Dönitz Nuremberg episode stands out as a failure of the law of war to keep pace with the realities of combat. As Nimitz's interrogatory made clear, states confronted with legal rules that reflect neither reality nor state practice suffer relegation to irrelevance, or provoke legal fictions.

In the context of CNAs, current applications of accepted legal standards for combatant status suffer similar detachment from reality. The

---

the enemy" explained the U.S. failure to rescue Japanese merchant seamen. *Id.* at 110.

261. 13 *id.* at 347 (1948).

262. *Id.* In his arguments on Dönitz's behalf, Kranzbühler highlighted early German compliance with the merchant vessel examination and rescue requirements. In particular, he touted examples of U-boat commanders towing rafts of shipwrecked crewmen to safety and the opportunity cost borne in lost attacks on lawful targets. *Id.* at 314.

263. 22 *id.* at 558. The Tribunal cited the British practice of arming merchant vessels and requiring merchants to report sightings of German submarines as the basis for the acquittal. *Id.* A later British Admiralty instruction directed British merchant ships to ram U-boats when possible. *Id.*

264. *Id.* at 559. The Tribunal found that the evidence did not clearly establish that Dönitz ordered attacks on surviving merchant crewmen. *Id.* The evidence did establish, however, that Dönitz ordered that the rescue provisions of the *Procès-Verbal* not be carried out. *Id.*

265. *Id.* at 559. The Tribunal sentenced Dönitz to ten years' imprisonment. *Id.* at 588. For his part, Dönitz expressed no regret over his conduct of the submarine campaign. In his final statement to the Tribunal, Dönitz said, "I consider this form of warfare justified and have acted according to my conscience. I would have to do exactly the same all over again." *Id.* at 390.

266. *See* DOENITZ AT NUREMBERG: A REAPPRAISAL 10 (H.K. Thompson, Jr. & Henry Strutz eds., 1976). Thompson and Strutz present critical comments on the International Military Tribunal from over 350 flag officers, justices, and statesmen. For example, British Air Vice-Marshal Hugh Champion de Crespigny offers: "Doenitz is no more guilty of a war crime than others on our side . . . . The unrestricted submarine warfare directed by Admiral Doenitz against Allied shipping was no more of a crime than Allied mass bombing of German towns and cities . . . ." *Id.*

four criteria traditionally required of the combatant class bear little relevance to the practices and requirements of CNAs. Only the more vaguely expressed principles behind the criteria, such as distinction and discipline, appear to be relevant to CNAs.

In the face of conflicting evaluations of the adequacy of existing law, state affiliation charts a course responsive to both textual and normative considerations. As a threshold for combatant status in CNAs, state affiliation enjoys solid textual support, appearing as a precondition in well over a century of positive law. In the same way that war evolved to render the Treaty of London criteria for merchant shipping attacks irrelevant, state practice has proved or soon will prove that the Geneva criteria are an outmoded test for evaluating combatant status in CNA. If the law of war is to continue to regulate the boundaries of the combatant class, resort to criteria tailored to the realities of combat should displace tradition-bound prerequisites. Normatively, state affiliation serves the long-standing principles of distinction and discipline among combatants, while doing so with minimal disruption to existing state practice. Further, adjusting the combatant threshold to account for the realities of CNAs may serve as a first step to reevaluating lawful participation in hostilities in other forms of remote warfare.